DEMOBOX DEPLOYMENT DOCUMENTATION

DEMONSTRATION AND DEPLOYMENT SCRIPT
CISCO MOBILITY EXPRESS WIRELESS DEMO VERSION 1.6

CCA version 1.6

TABLE OF CONTENTS

INTRODUCTION **3**

DEMONSTRATION GOALS 3
DEMONSTRATION SCRIPT STYLE 3

.... **3**

GENERAL PRESENTATION TIPS 3

CISCO MOBILITY EXPRESS WIRELESS NETWORK **4**

KEY FEATURES 6
MARKETING MESSAGES 6
HELPFUL URLS 7

CISCO AIRONET SERIES LIGHTWEIGHT ACCESS POINTS **8**

KEY FEATURES 8
MARKETING MESSAGES 9
DEMONSTRATION NOTES 10
DEMO ACTIONS 10
AP Registration *10*
KEY FEATURES 11

CISCO MOBILITY EXPRESS CONFIGURATION AND MANAGEMENT **12**

MARKETING MESSAGES 12
DEMONSTRATION NOTES 16
DEMO ACTIONS 16
Cisco Configuration Assistant Overview *17*
Configuring 526 Wireless LAN Controllers *34*
Auto Radio Frequency (RF) and Power Management *35*

MOBILITY EXPRESS SECURITY AND GUEST ACCESS **37**

KEY FEATURES 38
MARKETING MESSAGES 38
DEMONSTRATION NOTES 38
DEMO ACTIONS 38
Mobility Express Security Configuration *38*
Cisco Wireless Clients *40*
MARKETING MESSAGES 41
Client Failover *66*
Create Guest Web Authentication *71*
Web Authentication lockout *77*

APPENDIX-A — IP ADDRESSING AND ACCOUNT INFORMATION **78**

APPENDIX-B — CISCO CONFIGURATION ASSISTANT 1.6 .... **79**

APPENDIX-C — CISCO 500 SERIES WIRELESS MOBILITY EXPRESS CONTROLLER **88**

APPENDIX-D — CISCO 500 SERIES UNIFIED COMMUNICATION **92**

APPENDIX-E — CISCO CATALYST EXPRESS 520 SERIES SWITCHES **94**

INTRODUCTION

Welcome to the Cisco® Mobility Express Wireless Demo Box for small and medium-sized business (SMB) and midmarket customers. This kit is designed to provide you with everything you need to demonstrate a wide range of product features to a variety of potential customers, and illustrate the business benefits that Cisco Mobility Express Wireless solutions provide.

Demonstration Goals

The goal of this demonstration solution is to prove to customers that a Cisco Mobility Express Wireless solution is the best choice for their business. The demonstrations are designed to achieve the following:

- Customer awareness of what the solution can do
- Customer understanding of why the Cisco Systems® solution is unique, and the benefits of the Cisco solution relative to the status quo or competitive solutions
- Customer understanding of the Cisco solution purchasing and implementation process
- Appeal to the business decision maker (BDM) by focusing on the solution business impact

Demonstration Script Style

The Cisco Mobility Express Wireless DemoBox script uses a horizontal approach (feature-based) to show the feature elements. Each feature-based section includes important marketing messages as well as product and feature overviews and demonstration instructions. It is not intended that you select demo tasks based on customer requirements instead of perform every demo in this script. Present the demo's to your customers with vertical situations applicable to their needs and explanations based on their business requirements.

Demonstration Scripts Key

- Bulleted features in each script can be selected individually for demonstration.

STEP 1. Numbered instructions must be implemented in the order shown.

Note Important instructions!

General Presentation Tips

- Before you begin each demonstration scenario, explain what you are going to demo.
- Make the demo relevant by relating what you're demonstrating to the customer's specific situation. Communicate the appropriate relevant marketing messages.
- Explain what they will see and hear during the demonstration
- Perform the demonstration with only brief comments during the demonstration that help keep the customer oriented to the demo progress.
- After each demo is completed, recap what they saw and heard in the demo and reiterate the relevance to the customer's situation and why that's an improvement over their current operation (from customer/caller perspective as well as an agent/supervisor/corporate perspective). This is where the emphasize callouts can be used.
- Solicit feedback and impressions. Correct any erroneous impressions. Try to gauge the impact the demos have had on the customer's understanding of the benefits of the solution, its relevance to their company, and their vendor preference.

CISCO MOBILITY EXPRESS WIRELESS NETWORK

The Cisco Mobility Express Wireless Network is the industry's only Mobility Express wired and wireless solution to cost-effectively address the Wireless LAN (WLAN) security, deployment, management, and control issues facing SMB. This powerful solution combines the best elements of wireless and wired networking to deliver scalable, manageable, and secure WLANs with a low total cost of ownership. It includes innovative RF capabilities that enable real-time access to core business applications and provides proven enterprise-class secure connectivity. The Cisco Mobility Express Wireless Network delivers the same level of security, scalability, reliability, ease of deployment, and management for wireless LANs that organizations expect from their wired LANs.

Table 1 describes the demonstrations covered in this script.

Table 1. Mobility Express Wireless Demos

Demo	Device(s)/Product	Duration (min.)
Lightweight APs (LWAPP)	Cisco Access Points	5
Mobility Express WLAN Management	Cisco Wireless LAN Controller (WLC) and Cisco Configuration Assistant	10 - 15
Security	Cisco Wireless LAN Controller , CCA and UC520	10 - 15
Wireless Clients	Cisco Wireless Clients with variety of supplicants	15 - 20
Wireless VoIP	Cisco WLC 526 and UC 520 with 7921 and Nokia	10 - 15
Guest Access	Cisco WLC 526 and CCA, WebAuth and WebUI	10 - 15

Figure 1. Demo Topology.

Note CE 520 is optional and not required for this Demo. If CE 520 is not used in the demo please connect all the devices directly to the UC 520 Ethernet PoE ports.

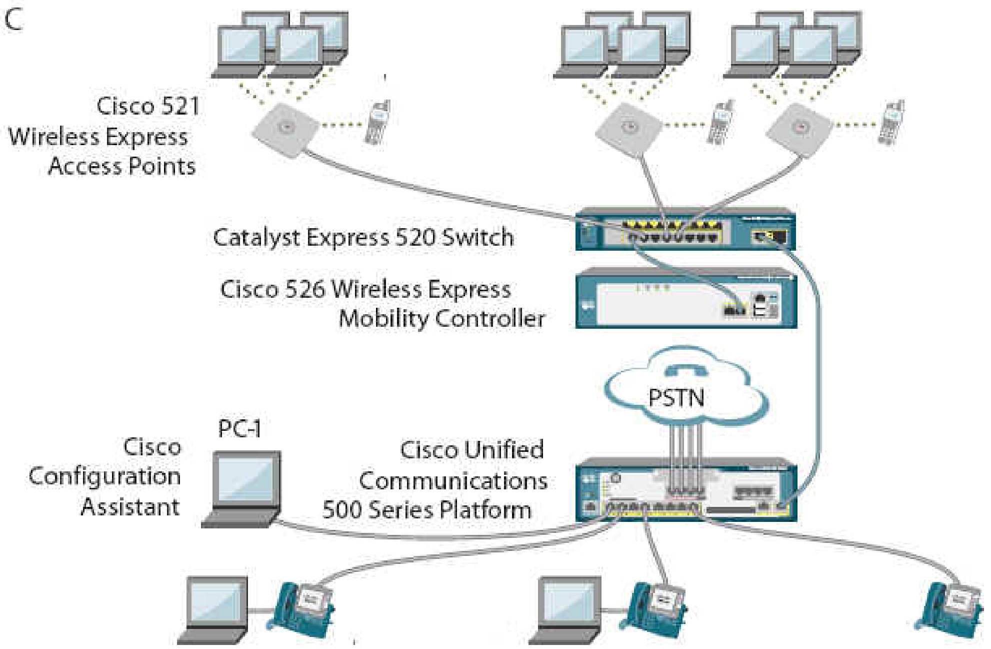

C
Cisco 521 Wireless Express Access Points
Catalyst Express 520 Switch
Cisco 526 Wireless Express Mobility Controller
PSTN
PC-1
Cisco Configuration Assistant
Cisco Unified Communications 500 Series Platform

Table 2. Devices

Device	Description
521 LWAPP Access Points	Cisco Aironet 521 Series 802.11/b/g Access Point w/Internal. Antennas
PC or Laptop	PC or laptop with Win XP and CCA ver 1.6
WL526 Controller	526 Series WLAN Controller for up to 6 Cisco lightweight APs per controller. Maximum two allowed.
UC520	Unified Communications 520 w/wireless option
CCA ver 1.6	Cisco Configuration Assistant ver 1.6
Intermec CN-3 (Optional)	Intermec PDA CN-3 CCX v4.0 compatible (optional)
Laptop Wireless Clients	Laptop Client devoices with CCX Wireless Card and CSSC, ACU, ADU, MZC and Odyssey supplicants
CE520 (Optional)	CE 520 eight port PoE switch
Cisco 7921 **Nokia E60-1 (optional)**	Cisco 7921 802.11a/b/g Wireless Phone Nokia E60-1 Dual Mode Wireless Phone

Key Features

The Cisco SBCS – Small Business Communication System is an integrated end-to-end solution that addresses all layers of the WLAN, from client devices and access points, to the network infrastructure, to network management, to the delivery of advanced wireless services integration and award-winning, worldwide, 24-hour product support. It delivers the industry's best wireless LAN security, innovation, and investment protection. It is the only solution to integrate innovative access point technology with an award-winning centralized configuration and management system, intelligent control and a wide array of interoperable Cisco Compatible client devices.

The Cisco Mobility Express Wireless Network helps reduce overall operational expenses by simplifying network deployment, operations, and management. With this solution up to 12 access points, six per one controller, can be easily managed from a centralized management console. The flexibility of the Cisco Mobility Express Wireless Network allows network managers to design networks to meet their specific needs, whether implementing highly integrated network designs or simple overlay networks.

SBCS system integrates Wireless and Wired Voice services in one easy CCA managed solution.

Marketing Messages

Challenge

A worldwide revolution is occurring in business. Wi-Fi enabled notebook computers are proliferating and driving the adoption of SMB WLANs. Unlike past technology advancements that were driven by technology professionals, the explosion of SMB WLANs is being driven by mobile users, traveling professionals, wireless applications, and advanced services like voice over IP (VoIP) over Wi-Fi. The acceleration of SMB adoption of WLAN technology is radically transforming business operations, the network edge, data centers, and centralized IT control.

Today's business climate requires anywhere, anytime connectivity. Mobility changes the way organizations do business. Real-time interaction, instant messaging, text paging, voice services, network access while traveling, and real-time network access in the office are transforming the business environment. In an increasingly competitive business environment, companies need fast responses and want immediate results.

WLANs are now business-critical. End users are embracing the freedom and flexibility of wireless connectivity, and business executives are recognizing the competitive advantage of business-critical mobile applications. Organizations are deploying WLANs to increase employee productivity, enhance collaboration, and improve responsiveness to customers.

The increasing need for anytime connectivity is creating new challenges for today's networking professionals, who must respond to the growing demand for WLANs in an era of tight budgets and reduced resources. These networking professionals are discovering that in the absence of a company sanctioned wireless network, employees are deploying their own unauthorized access points that put the entire network at risk.

Network managers need to protect their networks and deliver secure WLAN access for their organizations. They need a wireless infrastructure that embraces the unique attributes of radio frequency (RF) technology and effectively supports today's business applications. They need to keep their wired network secure while laying a foundation for the smooth integration of new applications that embrace wireless technology. Network managers need a WLAN solution that takes full advantage of existing tools, knowledge, and network resources to cost-effectively address critical WLAN security, deployment, and control issues.

Solution

The Cisco Mobility Express Wireless Network is the industry's only Mobility Express wired and wireless solution to cost-effectively address the WLAN security, deployment, management, and control issues facing SMB. This powerful solution combines the best elements of wireless and wired networking to deliver scalable, manageable, and secure WLANs with a low total cost of ownership. It includes innovative RF capabilities that enable real-time access to core SMB applications and provides proven enterprise-class secure connectivity. The Cisco Mobility Express Wireless Network delivers the same level of security, scalability, reliability, ease of deployment, and management for wireless LANs that organizations expect from their wired LANs.

The Cisco Mobility Express Wireless Network is an integrated end-to-end solution that addresses all layers of the WLAN, from client devices and access points, to the network infrastructure, to network management, to the delivery of advanced wireless services integration and award-winning, worldwide, 24-hour product support. It delivers the industry's best wireless LAN security, innovation, and investment protection. It is the only solution to integrate innovative access point technology with a centralized management and configuration system, intelligent control and a wide array of interoperable Cisco Compatible client devices.

The Cisco Mobility Express Wireless Network helps reduce overall operational expenses by simplifying network deployment, operations, and management.

Helpful URLs

Cisco SBCS on CCO

http://www.cisco.com/en/US/netsol/ns637/networking_solutions_market_segment_solutions_home.html

http://www.cisco.com/web/solutions/smb/products/voice_conferencing/smart_business_communications_system/index.html

Cisco Wireless Links for Customers

When demonstrating to Customers, please reference the websites for wireless related information:

http://www.cisco.com/go/wireless

CISCO AIRONET SERIES LIGHTWEIGHT ACCESS POINTS

Demo Time: 1 to 10 minutes

The Cisco Mobility Express Solution brings together the 521 Access Point and the Cisco 500 Series Wireless Express Mobility Controller to provide a flexible, cost effective wireless solution specifically designed to meet the needs of small and medium-sized businesses (SMBs). The Mobility Express Solution aligns with the Cisco Smart Business Communication System-a unified communications solution for SMBs that provides voice, data, video, security and wireless capabilities while integrating with existing desktop applications like calendar, e-mail and CRM to provide a complete solution.
As part of this solution, the Cisco 521 Access Point uniquely addresses the diverse requirements of small and medium-sized businesses (SMBs) by offering the versatility of operating either in standalone mode, or in controller-based mode with the Cisco 500 Series Wireless Express Controller.

Customers need wireless access points and clients which are easy to centrally manage, monitor, and secure the wireless network as well as minimize costs of deploying wireless access point and clients.

Note More information on Cisco wireless products can be found at www.cisco.com/go/wireless

Key Features

The Cisco® 521 Wireless Express Access Point is a single-band 802.11g access point that features business-class management, security, and scalability. This access point offers high-performance wireless connectivity in carpeted offices and similar environments.

Figure 2. Cisco 521 Wireless Express Access Points

http://www.cisco.com/en/US/products/ps7319/products_data_sheet0900aecd8060c220.html

SMB-class access point with integrated antennas for easy deployment in carpeted offices and similar RF environments.

• Standalone mode: Access points are directly connected to the wired infrastructure and provide reliable high-speed wireless connectivity to users in the area they cover. Configuration and management is performed locally at the individual access point level. Maximum of three standalone APs are supported.

• Controller-based mode: Access points associate with a Cisco 526 Series Wireless Express Controller to provide wireless connectivity and comprehensive monitoring of the airspace. The controller streamlines and manages the configuration of all connected access points through a single interface, instead of requiring configuration of each unit separately.

The Cisco 521 Access Point delivers optimal value for carpeted offices and similar environments. Built-in antennas provide omni-directional coverage specifically designed for today's open workspaces. A multipurpose mounting bracket easily secures Cisco 521 Access Points to ceilings and walls. With an unobtrusive design, the access points are aesthetically appealing and blend into their surrounding environment. For maximum concealment, they may be placed above ceilings or suspended ceilings. The access point's UL 2043 rating allows it to be placed above ceilings in plenum areas regulated by municipal fire codes. Offered at a competitive price point and optimized for easy installation and operation, the Cisco 521 Access Point helps organizations attain a lower total cost of ownership. Two 526 Wireless Mobility Express controllers and up to twelve Controller-mode 521 APs are supported.

Marketing Messages

Management (Lower Total Cost of Ownership)

The Cisco 521 Lightweight Access Points, which provide 802.11 b/g zero- touch configuration and management, deliver cost effective wireless access with advanced WLAN services for any deployment.

Security (Lower Risk)

This series of access points supports Wi-Fi Protected Access (WPA) and 802.11i/WPA2 for enterprise-class interoperable WLAN security.

- The APs support all the latest industry security standards to provide confidentiality, integrity and availability for the wireless network.
- If an AP is stolen, confidential information cannot be harvested from the AP since the configuration is stored in volatile memory, thus mitigating risk.

- The APs are dynamically configured for RF and power levels, thus minimizing cost to implement, operate, and optimize wireless coverage

Flexible and Easy Installation options (Lower Total Cost of Ownership)

Models are available with internal antennas. Cisco Aironet Lightweight Access Points support industry standard 802.3af Power over Ethernet (via PoE switch or injector). An external power supply is also available.

In offices and similarly open environments, Cisco 521 Wireless Express Access Points may be installed on the ceiling to provide users with continuous coverage as they roam throughout a facility. In school buildings and similar facilities, the access points may be installed on the ceiling of each room and hallway to provide users with full coverage and high network availability. In areas where a ceiling installation may not be practical, such as retail hotspots or similar small facilities, the access points can be mounted simply and securely on walls for complete coverage with minimal installation cost.

Demonstration Notes

When performing this demo, keep in mind that it will take several minutes for the APs to register back to the controller and update their status in CCA.

Demo Actions

AP Registration

STEP 1. Open CCA on the configuration PC or Laptop using the desktop shortcut. Login is <admin/cisco>

STEP 2. In CCA, go to **MONITOR> Wireless Radios** > **Refresh**.

STEP 3. On the screen you should see all access points, their names, MAC addresses, channel assignments and transmit power

Note The 521 APs should be setup in a six foot by six foot grid with WLC 526 and UC 520 in the middle

STEP 4. Unplug one of the APs. Pass these around to customers. When they are finished, have them plug the AP into the appropriate Ethernet cable. It will take several minutes before the AP will be removed from the topology view. When clicking on the **Inventory** button on the menu, removed AP should not be on the list.

STEP 5. Point out that no other tasks are required on the AP to replace or add APs. Everything is managed from the CCA 1.6.

Note Configuration and maintenance is not performed on the AP itself. (Zero-touch configuration).

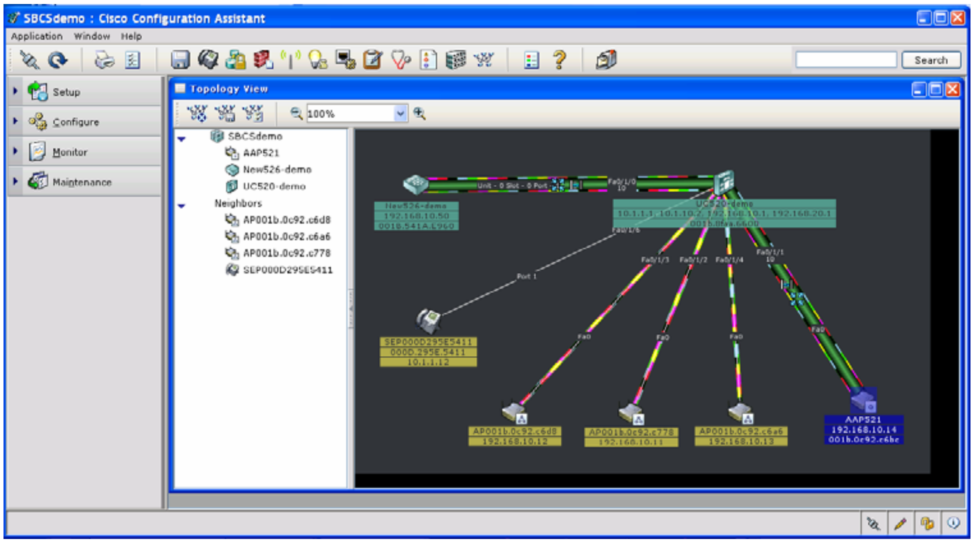
Polling intervals can be adjusted from the Main Menu on the top bar. Topology view and options can be adjusted from the menu in the topology window.

STEP 6. While the APs reload, point out the APs which are receiving the operating system and configuration from the Wireless LAN Controller. Once the 521 LAP is registered, solid LEDs for the power (green) will be displayed for Registered AP

STEP 7. Return to the CCA Topology screen and verify there are 3 APs registered (or as many as available). If only 2 APs are registered, click the refresh button to see the third. This process again may take several minutes.

STEP 8. Now go to **Monitor** > **Wireless Clients** and you should see all the wireless clients registered to the APs

STEP 9. Show the customer that LAP 521 or controller-mode AP icon has a triangle and the AAP or stand alone AP icon has a circle.



Key Features

CISCO MOBILITY EXPRESS CONFIGURATION AND MANAGEMENT

Demo Time: 15 to 25 minutes

Wireless is a rapidly changing environment; managing this change is challenging in most wireless deployments. To resolve this problem, changes to the APs, such as RF and power levels, are made dynamically by the controllers. Other changes require manual changes. Cisco makes these manual changes possible from the controller WebUI or in the Mobility Express solution using CCA (Cisco Configuration Assistant), minimizing or eliminating repetitive tasks of updating individual access points. In the next several Mobility Express releases most or all configuration options will be available from CCA. Making changes using CCA are more effective and easier to understand and implement. Most of the CLI interfaces are disabled in the Mobility Express systems; only advanced and show commands are still available via the CLI.

The components highlighted in this demo section are shown in Table 3.

Table 3. Key Components of Cisco's Mobility Express WLAN Management

Demo	Description
Cisco Configuration Assistant	CCA is the industry leading platform for wireless LAN configuration and management of multiple WLAN controllers, Unified Communication 520, Catalyst Express 500 series and stand alone APs.
WLAN Controller (WLC)	Cisco Wireless LAN Controllers are responsible for system wide wireless LAN functions, such as security policies, intrusion detection, RF management, quality of service (QoS), and mobility. They work in conjunction with Mobility Express Lightweight Access Points using the Lightweight Access Point Protocol (LWAPP).
UC 520	UC 520 –is an easy-to-deploy solution smoothly integrates with Cisco Wireless LAN Controllers and Cisco lightweight access it provides additional services required for wireless deployment, such DHCP and AAA services.

The demos covered in this section are shown in Table 4.

Table 4. Management Demos

Demo	Duration (min.)	Description
Component Overview	5	WLAN Controller, CCA and UC520
WLC 526 configuration	10	WLAN 526 controller
Auto RF using WebUI	3	Dynamic Power Control, Dynamic Channel Control (install/setup), Dynamic Channel Control
CCA overview	15	CCA version 1.6 and WLC updated with the latest software release

Marketing Messages

Cisco Configuration Assistant

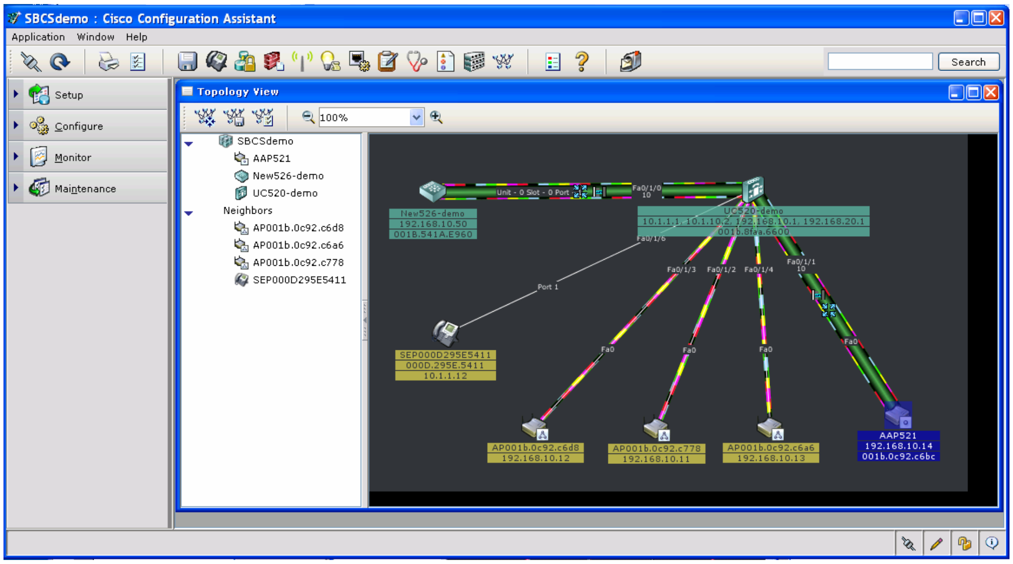
Cisco Configuration Assistant, a PC-based intuitive GUI configuration tool, is an integral component of the Cisco Smart Business Communications System. With a focus on ease of use, the Cisco Configuration Assistant simplifies configuration of multiple

technologies-unified communications, switching, routing, security, and wireless. Cisco Configuration Assistant simplifies wireless configuration and provides follow-up support to facilitate easy modification. Features include an interactive topology view, front-panel views of devices, and drag-and-drop Cisco IOS Software upgrades.
Cisco Configuration Assistant was purpose-built to provide comprehensive configuration, deployment, and ongoing network management support for the entire line of products in the Cisco Smart Business Communications System.

Cisco Configuration Assistant Key Features

Cisco Configuration Assistant provides the following features and benefits:
• Holistic, network-level insight through multiple network views-Users can access devices and monitor the network from two perspectives: the physical Topology View or the Front Panel View. The rich Topology View graphically represents the types of devices in the network as well as detailed information about device status, physical connections, and various monitoring capabilities-all from a single view. The Front Panel View displays all switches, controllers and routers in the network simultaneously, along with the state, duplex, and speed of ports. The Front Panel View also allows users to apply features across multiple ports or multiple switches when configuring features such as VLANs. In addition, users can verify optimal ongoing network performance by generating comprehensive, real-time reports of network inventory and health.

Figure 7. The Topology View graphically represents the types of devices in the network and provides detailed information about device status and physical connections



• Simplified topology mapping and deployment through dynamic discovery-Cisco Configuration Assistant's unique discovery capabilities provide users with total control when discovering network devices to create a community. Users can discover devices by entering a seed IP, range IP, subnet IP, or a single IP address. This feature provides more flexibility and time savings when designing the topology.

• Clear separation of services through VLAN highlighting-From the Topology View, users can associate VLAN numbers with colors to quickly view what devices are in a VLAN. Devices that are associated with more than one VLAN display two or more colors with a striped effect.

• Customization with annotated text-Users can add additional text under devices in the Topology View to further describe aspects of the network, such as the name of a building, floor, or closet.

• Improved network visibility with continual health monitoring-Users can quickly assess the status of switches and routers, including packet errors; temperature; PoE status; and bandwidth, CPU, memory, and ternary content addressable memory (TCAM) usage-all from a single window. Users can select the specific health categories to monitor. For each category selected, the switch with the highest usage is displayed in the quick view. Users can access a more comprehensive view by clicking the "Details" button.

- Simplified network reporting-Users can print easy to read reports such as bandwidth utilization. The enhanced print option even allows users to print the Topology View or Front Panel View on one page using the "fit to page" option.
- Enhanced security for configuration and monitoring activities-Cisco Configuration Assistant provides a secure connection between the Cisco Configuration Assistant client and each connected device in the network to safeguard all sensitive information.
- Increased IT staff efficiency through simplified software updates-The drag-and-drop Cisco IOS Software Upgrade feature simplifies the process of upgrading the Cisco IOS Software on a Cisco Catalyst® switch or Cisco router or access point. Users can download the latest software version by simply dragging the update's icon from the PC desktop and dropping it onto the icon of the target device depicted in the Topology View. This process eliminates the need to use the specific Cisco IOS Software filename or select a specific Trivial File Transfer Protocol (TFTP) server IP address when performing updates. This process can also be use to deploy Cisco Unified Express images, phone loads, music on hold files and language packs onto the router.
- Improved network security and performance with dynamic application updates-Users can stay up-to-date on the latest versions and security patches of Cisco Configuration Assistant through dynamic application updates. With this function, users can be assured that when a newly purchased Cisco device is added to the network, it is automatically supported and secured with the latest update.
- Enhanced ability to identify and address issues-The Event Notification feature alerts users if a potential problem arises with a device in the network, if a configuration change is required, or if a new version of Cisco Configuration Assistant is available for download. A dialog box provides all necessary information regarding the event, including time; description; and, if applicable, suggestions to resolve the problem.
- Enhanced productivity of partners and guests-Cisco Configuration Assistant's Guest Port feature allows businesses to easily configure guest access ports on their switch, providing visiting guests with Internet access and allowing them to establish VPN connectivity to their company resources. Guest Port users are separated from internal network traffic so that confidential "internal access only" information and services remain secure from unauthorized guest users.
- Increased security and performance through network synchronization-This feature detects inconsistent settings in the network such as VLAN mismatches, centralized time, and security policies. Working with the Troubleshooting Advisor, users can detect and fix these inconsistencies easily.
- Simplified troubleshooting-Embedded in the application is the Troubleshooting Advisor, which simplifies troubleshooting by automatically identifying potential network problems and documenting them with a graphical trend chart. Examples include cabling problems, configuration errors, and other potential network problems. Users receive an explanation of the issue and often can correct the problem with a simple mouse click.
- Enhanced IT staff effectiveness through comprehensive online support-A detailed, transparent help function embedded in Cisco Configuration Assistant provides an extensive glossary and powerful search engine that help users quickly and easily find the information they need to apply specific settings. With these online help features, users often can troubleshoot and resolve problems without having to call for technical support.
- Faster network configuration and improved network performance through intelligent port configuration-Cisco Configuration Assistant includes the Cisco Smartports Advisor, which discovers devices connected in the network and recommends appropriate Cisco best practice configurations for security, availability, and QoS features on switch ports. This feature saves time by proactively recommending Cisco best practices and removes the need for network administrators to consult detailed design guides or documentation. The feature allows network administrators to configure ports more quickly; eliminates human error; and helps ensure the configuration of the switch, router, or access point is optimized for the business' applications.
- Improved IT staff efficiency and effectiveness when securing the network-Users can centrally configure security and access for Cisco Catalyst switches. Users simply choose the desired level of security (low, medium, or high) on the Security Slider in Cisco Configuration Assistant. The low setting (default) provides port security and protection against broadcast storms. The medium setting adds MAC address authentication. The high setting adds IEEE 802.1x authentication for media-level access control, providing the capability to permit or deny network connectivity and control VLAN access based on user or machine identity.

Cisco 500 Series Wireless Mobility Express Controller

The Cisco 500 Series Wireless Express Mobility Controller is designed to optimize the wireless networks of small and medium-sized businesses (SMBs). As a core element of the Cisco Mobility Express Solution, the mobility controller is built to specifically support the Cisco 500 Series Wireless Express Access Points. Together, they provide IT Managers complete visibility of the wireless network. The mobility controller automatically manages access points to reduce interference, avoid coverage gaps, maximize available bandwidth to ensure overall optimal network performance, and support advanced mobility services such as guest Internet access and voice over Wi-Fi.

Figure 3. 500 Series Controllers

The Cisco 526 Wireless Express Mobility Controller can be used with up to six access points per controller and up to two controllers per network. It harnesses the power of Cisco Lightweight Access Point Protocol (LWAPP) technology-best-in-class automatic radio optimization, mobility performance and multi-access-point management-at the capacity, simplicity, and price point appropriate for the SMB. On top of the basic transport layer, this controller supports Cisco Secure Guest Access and voice-over-WLAN advanced mobility services. Along with other products in the Smart Business Communications System, this controller uses the Cisco Configuration Assistant software rather than a command-line interface, accelerating deployment and decreasing the cost of ongoing maintenance.

Features and Benefits

Table 4 describes the features and benefits of the Cisco 526 Wireless Express Mobility Controller.

Table 4. Features and Benefits of the Cisco 526 Wireless Express Mobility Controller

Features	Benefits
Part of the Cisco Smart Business Communications System	Part of a portfolio of switching, routing, security, and voice products designed to work both individually and together as a multiproduct system to maximize the value of each product in the network.
Simplifies multi-access-point networks	Addresses issues in multi-access-point infrastructures, including scalable security, radio self-interference, and repetitive management tasks, to help ensure that multi-access-point networks operate at peak efficiency.
Streamlined management tool	Uses Cisco Configuration Assistant management software instead of a command-line interface for configuration to accelerate new and incremental deployments.

Supports Cisco LWAPP	Uses Cisco LWAPP for communication between access points and controllers to simplify deployment and follow-on management, and to automate functions required for a pervasive WLAN end-user experience.
Multi-access-point Radio Resource Management (RRM)	In builds with more than one access point, RRM coordinates access points in real time to optimize radio coverage/capacity while working around potential points of interference.
Secure authentication mechanism support	Support for a wide range of authentication mechanisms to enable scalable security architectures and minimize security interoperability issues (WEP, MAC Filtering, WPA, WPA2, WebAuth, and EAP).
Wired/wireless network virtualization	Supports the use of up to eight SSID/VLANs so that one physical WLAN infrastructure can be safely shared by different users, applications, or organizations as virtual wired/wireless networks.
Supports Cisco Secure Guest Access	With Secure Guest Access, organizations can create a virtual guest network with a Web login page for non-employees to get Internet access while safely partitioned from the sensitive corporate LAN.
Supports Cisco voice-over-WLAN optimization	Voice over WLAN optimization is a package of features that deliver quality of service, call admission control, and fast inter-access point hand-off to improve the quality of a wireless voice infrastructure.

Architectural Feature Comparison

With Cisco 521 Wireless Express Access Points, the Cisco Wireless Mobility Solution is an ideal fit for the SMB environment. Table 5 highlights the main architectural feature differences between consumer-grade, business-grade, and enterprise-grade WLAN solutions.

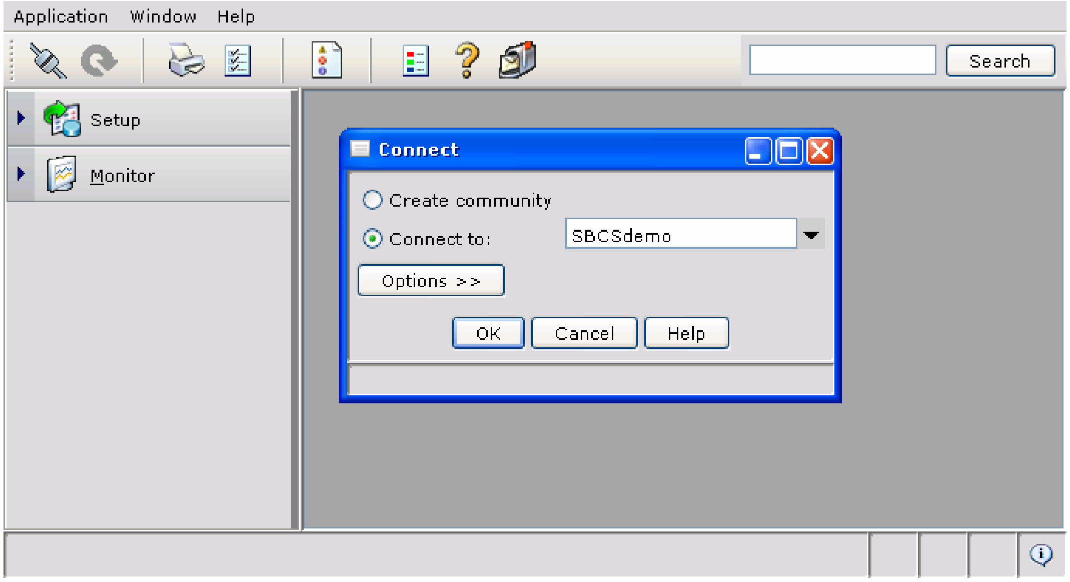
Demonstration Notes

WLC 526 is accessible using the desktop shortcut (local machine) or https://192.168.10.50 for remote machines. Configuration is done from the CCA and Web UI. CCA can be started by clicking the icon on the desktop.

Demo Actions

Cisco Configuration Assistant Overview

STEP 1. From the PC running CCA double click on the CCA icon on the desktop. The screen will come with the message to connect to community or create community. If community was already created then choose that community from the drop down menu. In our demo the community name is SBCS demo.

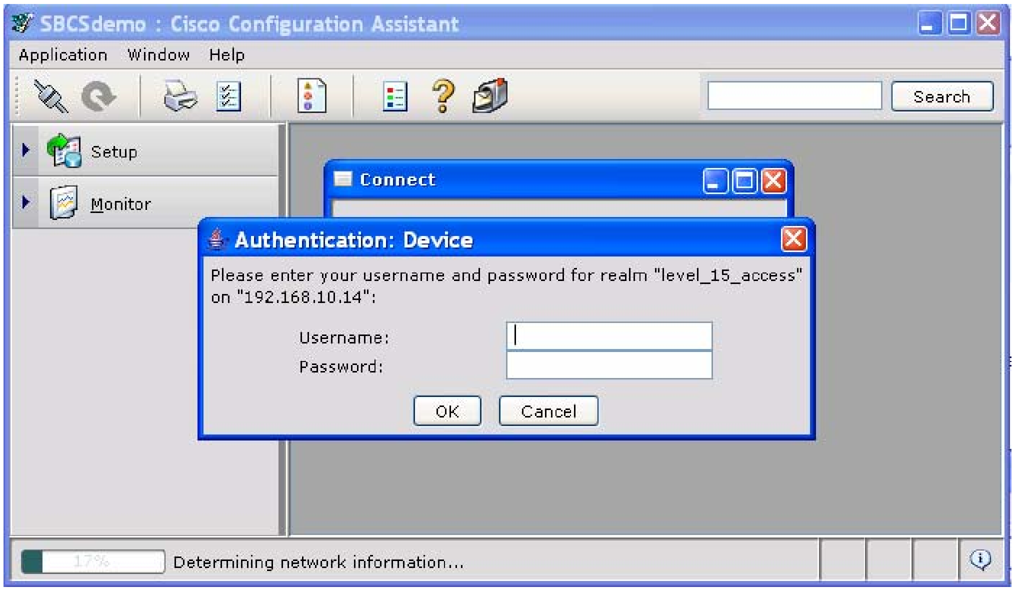


○ Create community

● Connect to: SBCSdemo

STEP 2. Click OK to connect to the community

STEP 3. The message will come up and ask for user name and password on the UC 520 our seed device address. Key in user name "**admin**" and password "**cisco**" and click OK. You may also see the screen that will ask you to accept the security certificates of the devices – please enter "yes" on that screen.

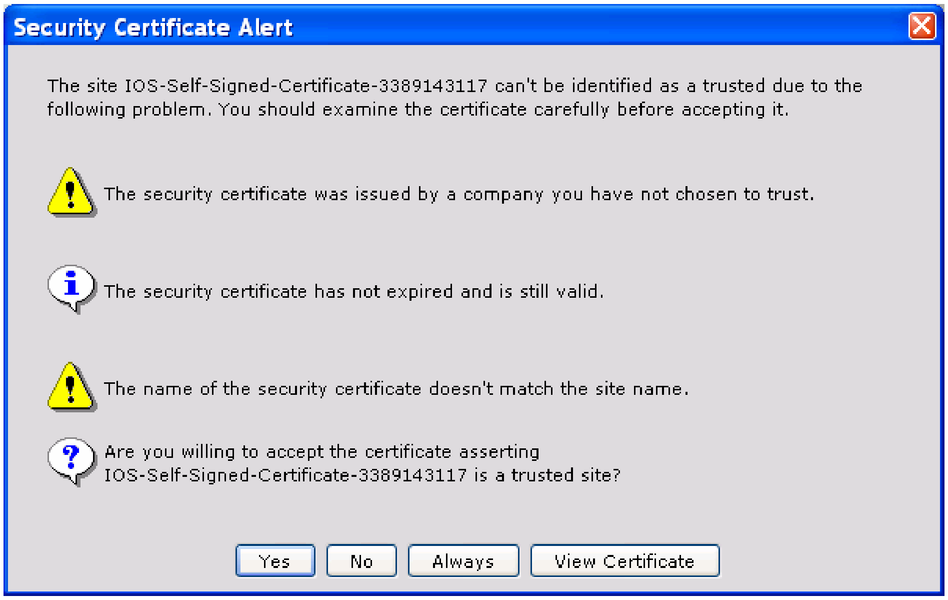


Please enter your username and password for realm "level_15_access" on "192.168.10.14":

Determining network information...

Note You might have other devices in the topology that will require different user name and passwords. You will need to know their default or administratively changed credentials for the CCA to be able to configure and manage them.

STEP 4. I f the community was not created then choose an option of creating community. In our demo we will create community "**SBCSdemo**" with the "seed IP address" of the UC 520. Enter the information indicated above and start discovery. After few seconds the devices will be discovered on the screen with their IP addresses and Host names. Again as before enter username and password "admin" and "cisco" and accept security certificates as they popup on the screen during the discovery process.



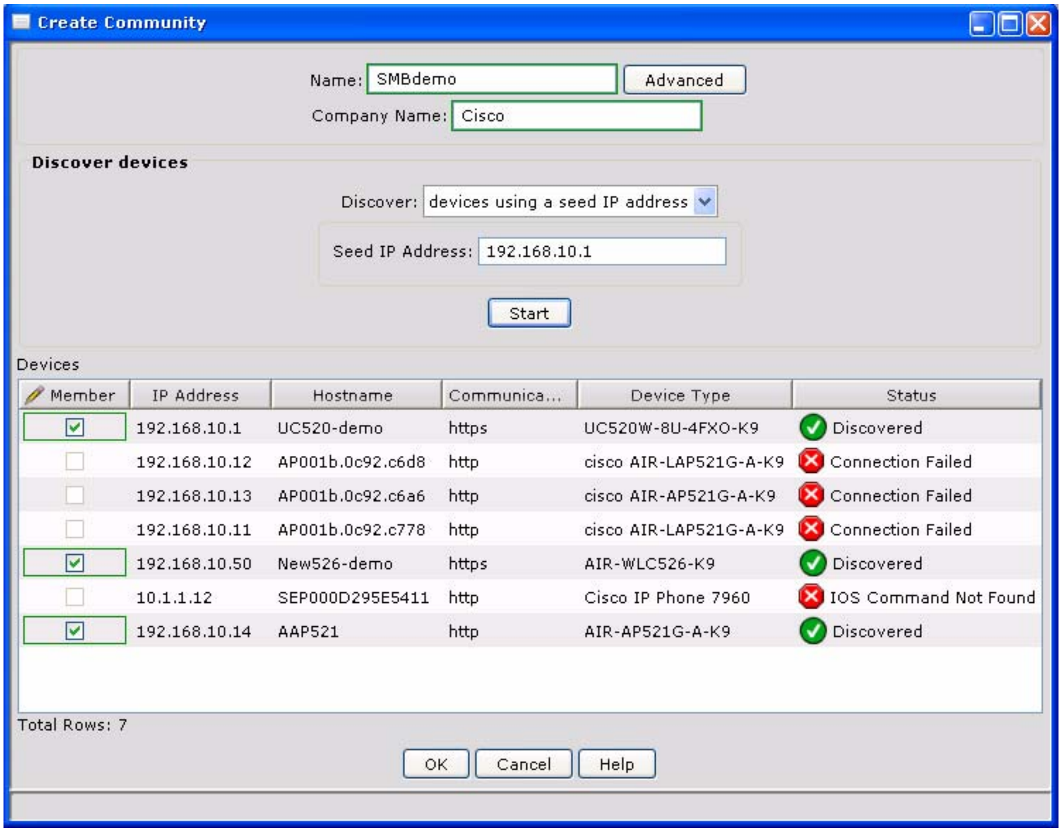
The site IOS-Self-Signed-Certificate-3389143117 can't be identified as a trusted due to the following problem. You should examine the certificate carefully before accepting it.

The security certificate was issued by a company you have not chosen to trust.

The security certificate has not expired and is still valid.

The name of the security certificate doesn't match the site name.

Are you willing to accept the certificate asserting IOS-Self-Signed-Certificate-3389143117 is a trusted site?



Create Community

Name: SMBdemo [Advanced]

Company Name: Cisco

Discover devices

Discover: devices using a seed IP address

Seed IP Address: 192.168.10.1

[Start]

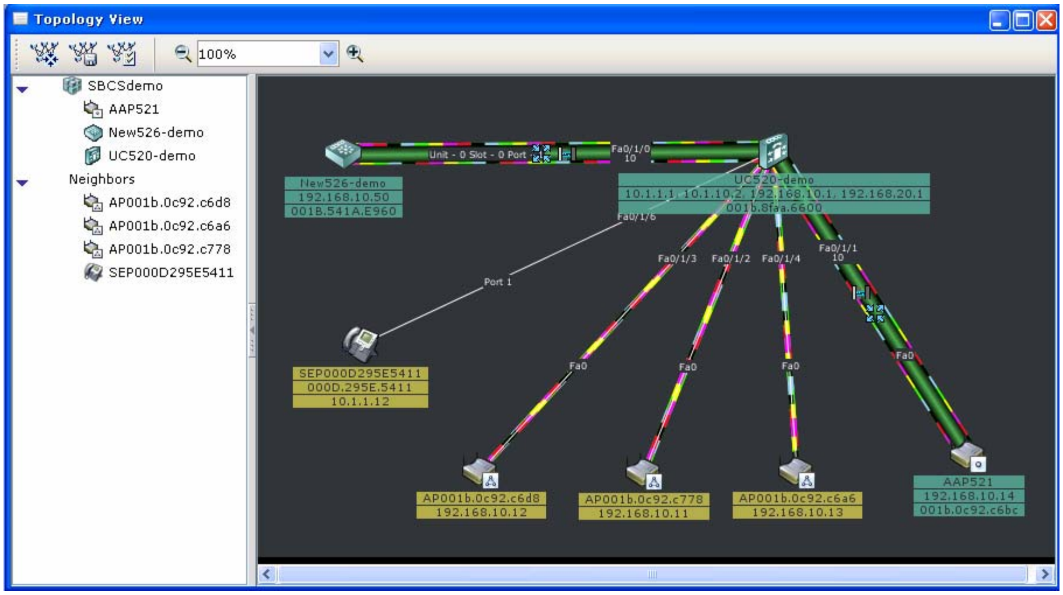
Devices

Member	IP Address	Hostname	Communica...	Device Type	Status
☑	192.168.10.1	UC520-demo	https	UC520W-8U-4FXO-K9	✓ Discovered
□	192.168.10.12	AP001b.0c92.c6d8	http	cisco AIR-LAP521G-A-K9	☒ Connection Failed
□	192.168.10.13	AP001b.0c92.c6a6	http	cisco AIR-AP521G-A-K9	☒ Connection Failed
□	192.168.10.11	AP001b.0c92.c778	http	cisco AIR-LAP521G-A-K9	☒ Connection Failed
☑	192.168.10.50	New526-demo	https	AIR-WLC526-K9	✓ Discovered
□	10.1.1.12	SEP000D295E5411	http	Cisco IP Phone 7960	☒ IOS Command Not Found
☑	192.168.10.14	AAP521	http	AIR-AP521G-A-K9	✓ Discovered

Total Rows: 7

[OK] [Cancel] [Help]

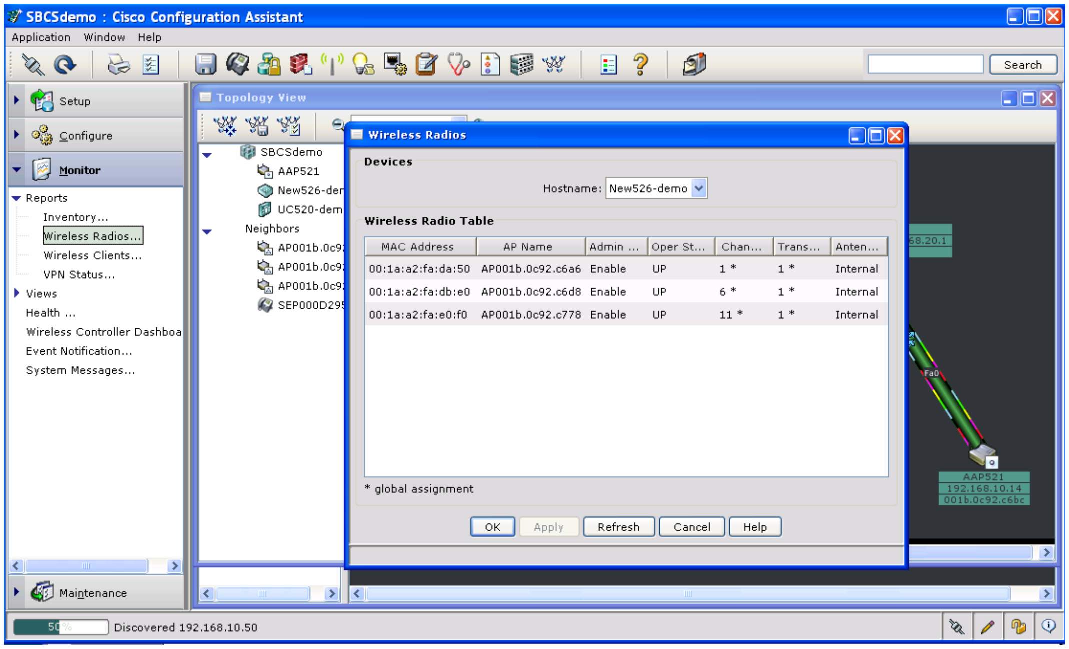
STEP 5. The CCA will come on the screen with Topology View of the configured network. Please make sure all the devices are discovered and presented on the Topology View screen.



Verify AP Registration

STEP 1. In the topology view verify that all the components are present and all the devices show MAC address and IP addresses. You can change the setting of what is shown on the screen in the Topology Preference Setting.

STEP 2. Open the **Monitor>Reports> Wireless Radios** menu and see all the APs connected to the controller and their Channel and Transmit power assignments.



Devices

Hostname: New526-demo

Wireless Radio Table

MAC Address	AP Name	Admin ...	Oper St...	Chan...	Trans...	Anten...
00:1a:a2:fa:da:50	AP001b.0c92.c6a6	Enable	UP	1 *	1 *	Internal
00:1a:a2:fa:db:e0	AP001b.0c92.c6d8	Enable	UP	6 *	1 *	Internal
00:1a:a2:fa:e0:f0	AP001b.0c92.c778	Enable	UP	11 *	1 *	Internal

* global assignment

Discovered 192.168.10.50

Note The AP Mac address entries will vary in every demo. Channels and Transmit power may be different as well

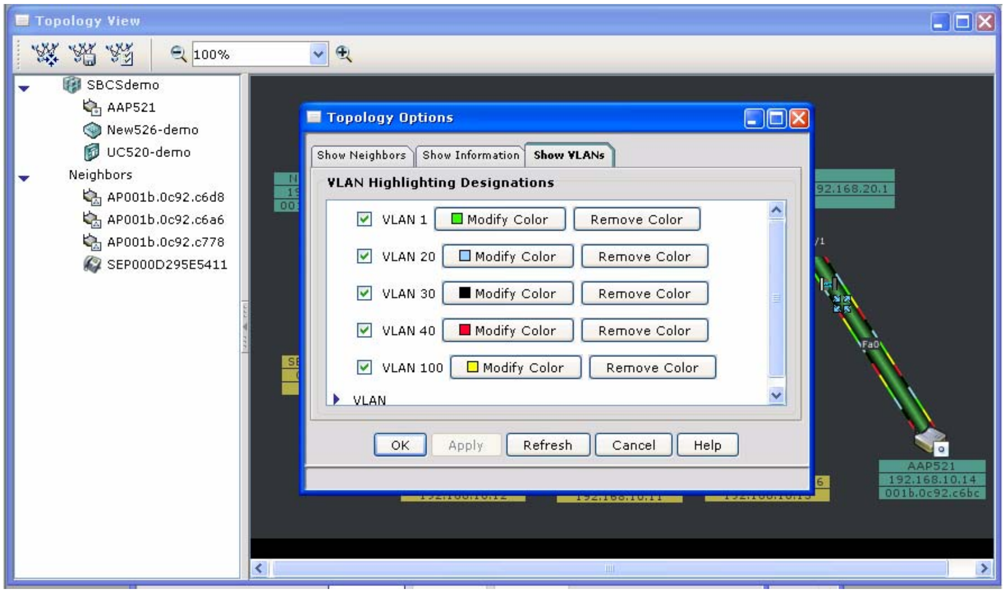
Verifying Clients Association

STEP 1. On the left side pull down menu choose **Monitor>Reports>Wireless Clients** and you will see all the Wireless clients associated and authenticated to the APs.

CCA features on the Topology View Screen

STEP 1. Double click on any Device icon on the screen and see the detailed device information or you can change devices name, get code version loaded on the device and write annotations.

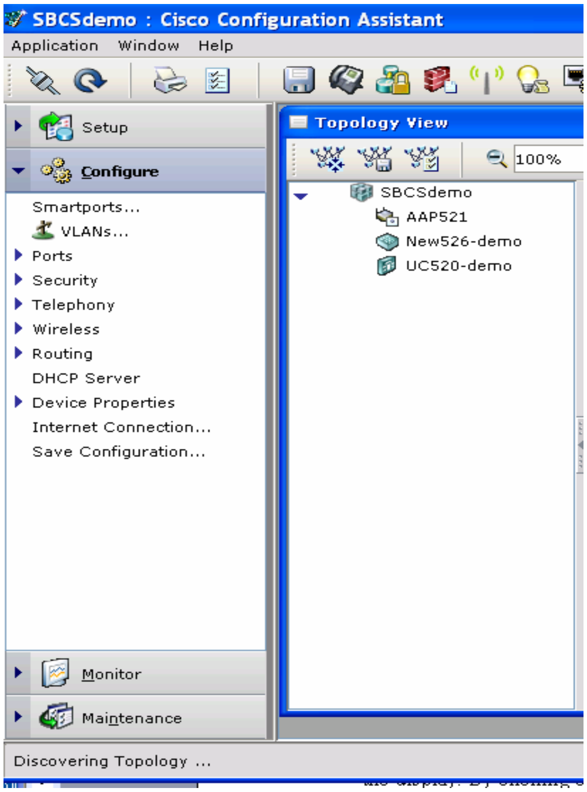
STEP 2. On the top menu of the Topology view there are Topology Icons for Changing layout, Saving Topology or Topology Options. One of the nice features is the ability to set colors for the VLAN of the SBCS network.



☑ VLAN 1 🟩
☑ VLAN 20 🟦
☑ VLAN 30 ■
☑ VLAN 40 🟥
☑ VLAN 100 🟨

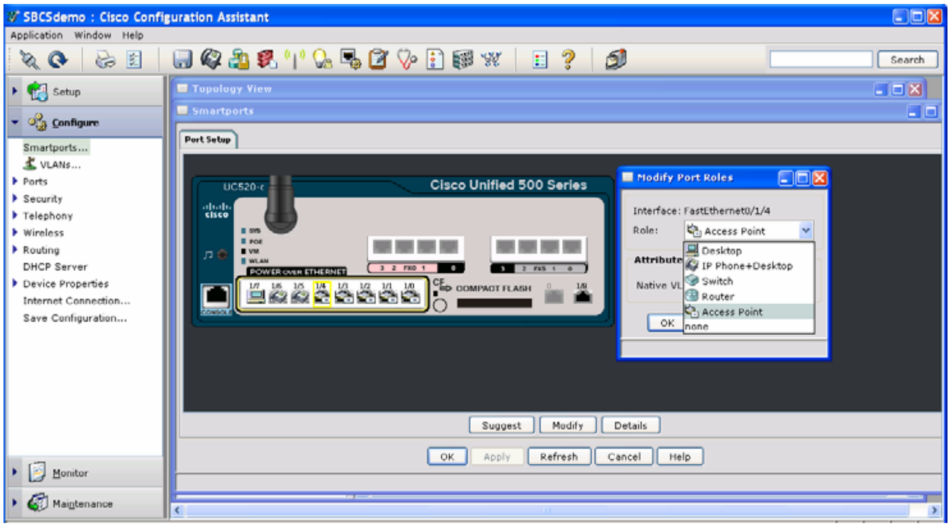
CCA menu options on the Left Side Menu

STEP 1. On the left side menu open the **Configure Tab** and view all the different options to configure Smartports, VLANs, Ports, Security, Telephony, Wireless, Routing, DHCP Server, Device Properties, etc.



Discovering Topology ...

STEP 2. Open the <**Configure**>< **Smartports** menu tab, you will see the UC500 displayed on the screen with Ethernet Smartports highlighted on the display. By clicking on the **Port** and then on the **Modify** button will show the configuration options for the port. Note that in our demo the port where the APs are connected configured as **Access Point** ports with default VLAN.

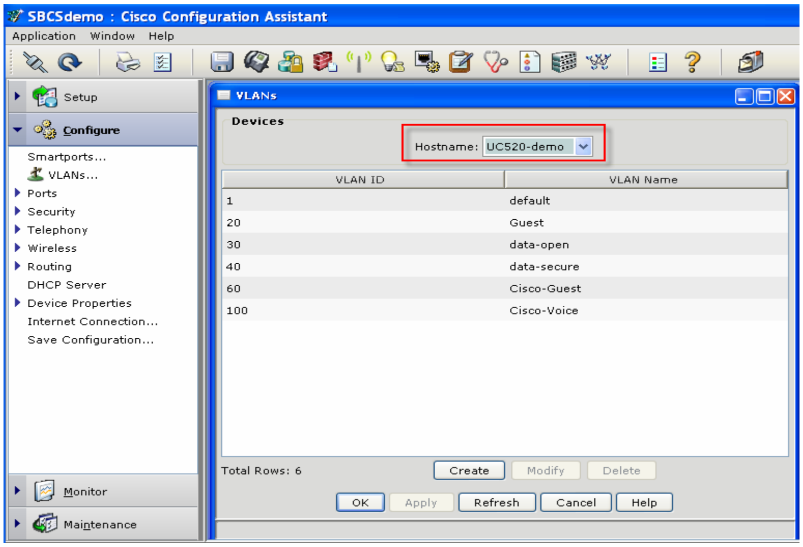


Interface: FastEthernet0/1/4

Role: Access Point

- Desktop
- IP Phone+Desktop
- Switch
- Router
- Access Point
- none

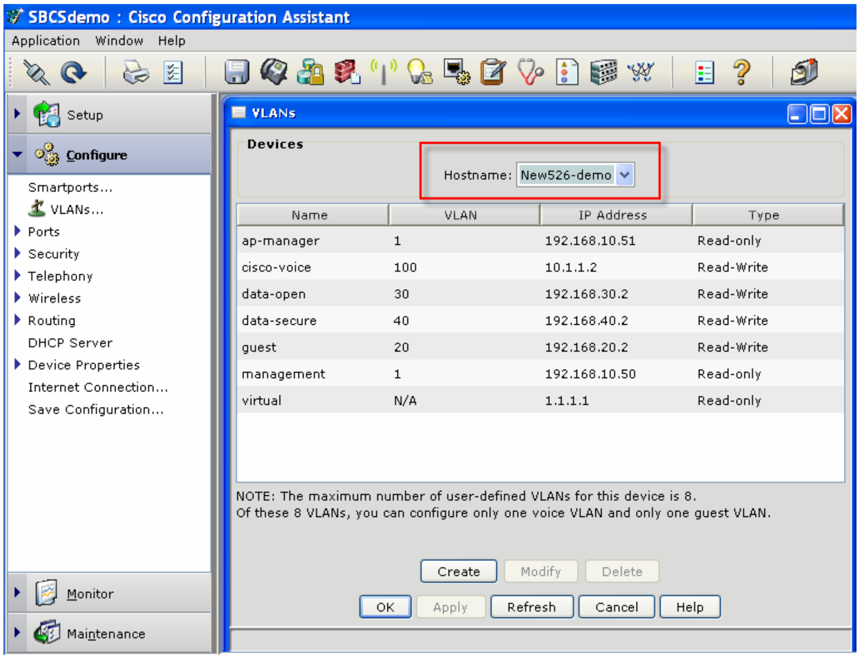
STEP 3. Next in the **Configure** menu choose **VLANs** – you will see VLANs configured on our network under the hostname UC520-demo and hostname New526-demo



Hostname: UC520-demo

VLAN ID	VLAN Name
1	default
20	Guest
30	data-open
40	data-secure
60	Cisco-Guest
100	Cisco-Voice

Total Rows: 6

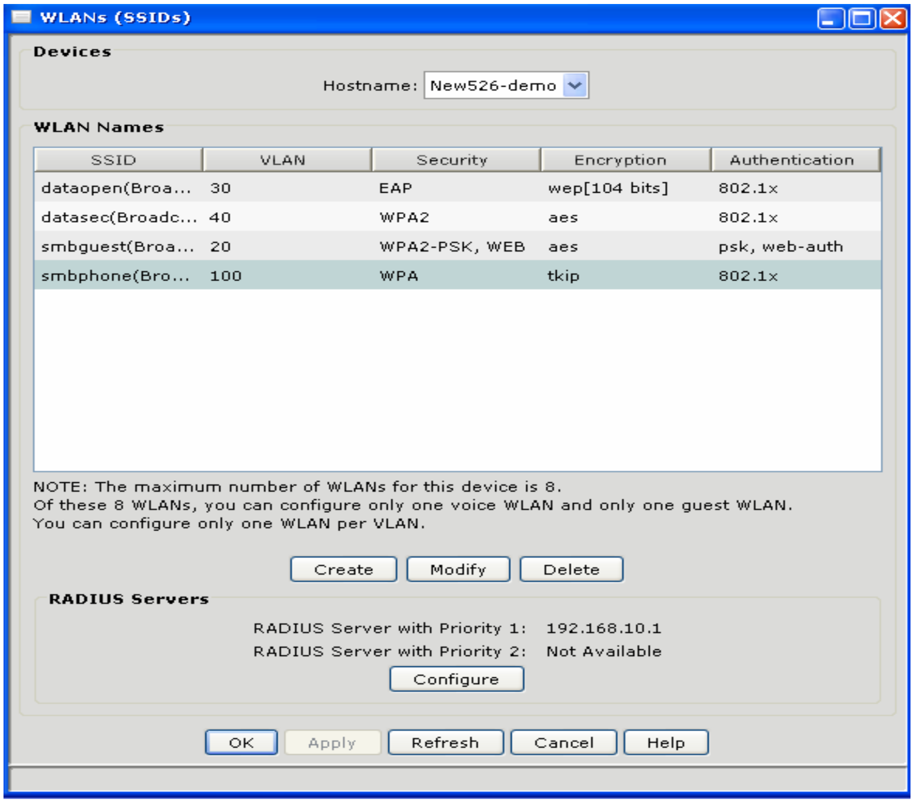


Hostname: New526-demo

Name	VLAN	IP Address	Type
ap-manager	1	192.168.10.51	Read-only
cisco-voice	100	10.1.1.2	Read-Write
data-open	30	192.168.30.2	Read-Write
data-secure	40	192.168.40.2	Read-Write
guest	20	192.168.20.2	Read-Write
management	1	192.168.10.50	Read-only
virtual	N/A	1.1.1.1	Read-only

NOTE: The maximum number of user-defined VLANs for this device is 8.
Of these 8 VLANs, you can configure only one voice VLAN and only one guest VLAN.

STEP 4. Next move on to the **Wireless Networks** and choose Hostname of the 526 controller, you will see all the SSIDs created and their security settings and VLANs they are assigned too. You can create a new SSID from this menu option as well.



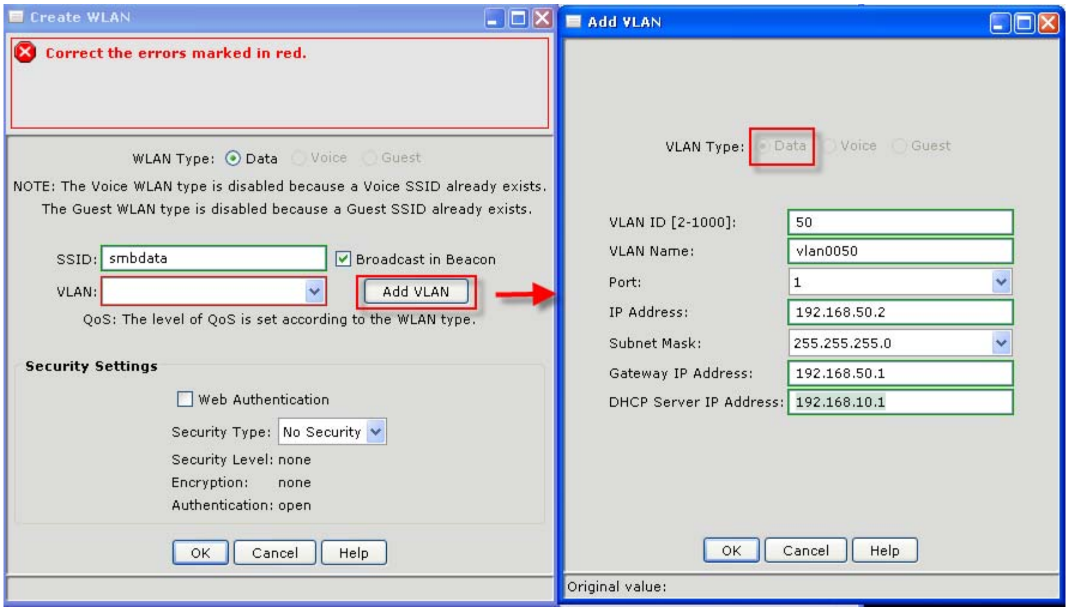
Hostname: New526-demo

SSID	VLAN	Security	Encryption	Authentication
dataopen(Broa...	30	EAP	wep[104 bits]	802.1x
datasec(Broadc...	40	WPA2	aes	802.1x
smbguest(Broa...	20	WPA2-PSK, WEB	aes	psk, web-auth
smbphone(Bro...	100	WPA	tkip	802.1x

NOTE: The maximum number of WLANs for this device is 8.
Of these 8 WLANs, you can configure only one voice WLAN and only one guest WLAN.
You can configure only one WLAN per VLAN.

RADIUS Server with Priority 1: 192.168.10.1
RADIUS Server with Priority 2: Not Available

Note If you choose to create a new SSID and there is no unassigned VLANs available the system will prompt you to first create a new VLAN for that SSID since Mobility Express system supports only one to one mapping between VLAN and SSID. See the Note on the screen capture above.



Correct the errors marked in red.

WLAN Type: ● Data ○ Voice ○ Guest

NOTE: The Voice WLAN type is disabled because a Voice SSID already exists.
The Guest WLAN type is disabled because a Guest SSID already exists.

SSID: smbdata ☑ Broadcast in Beacon

VLAN:

QoS: The level of QoS is set according to the WLAN type.

Security Settings

□ Web Authentication

Security Type: No Security

Security Level: none

Encryption: none

Authentication: open

VLAN Type: ● Data ○ Voice ○ Guest

VLAN ID [2-1000]: 50

VLAN Name: vlan0050

Port: 1

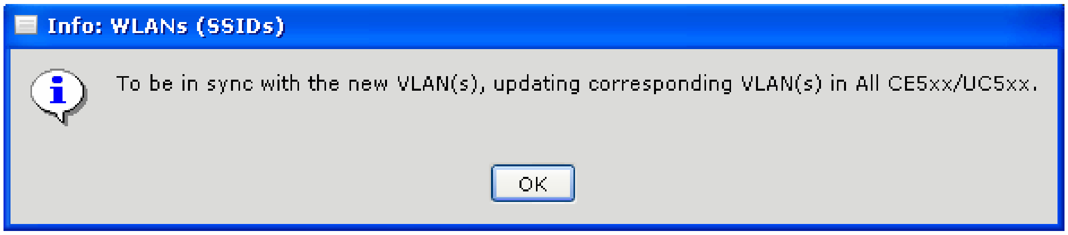
IP Address: 192.168.50.2

Subnet Mask: 255.255.255.0

Gateway IP Address: 192.168.50.1

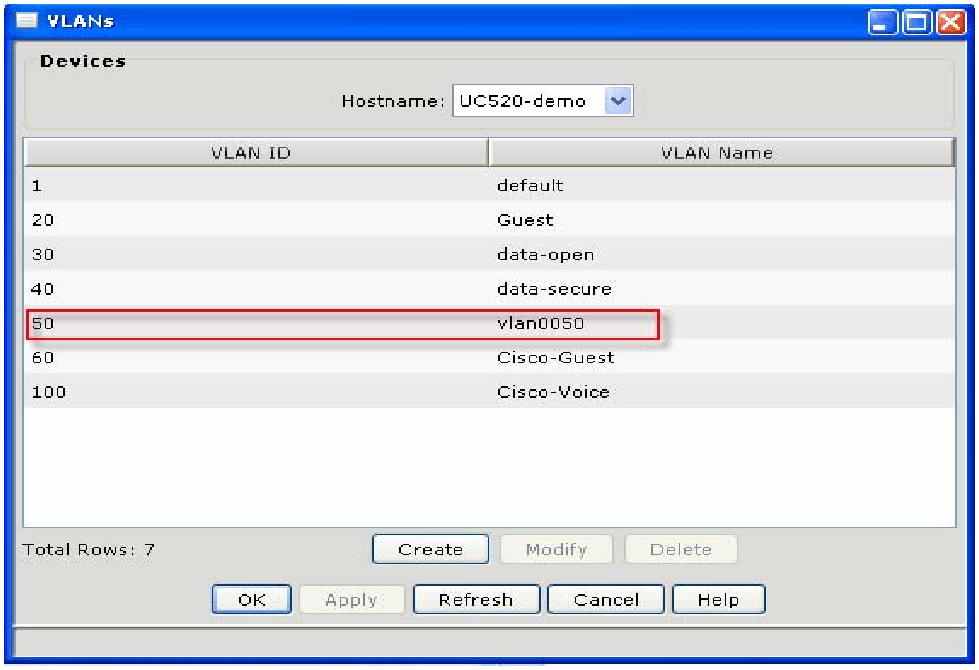
DHCP Server IP Address: 192.168.10.1

Original value:



To be in sync with the new VLAN(s), updating corresponding VLAN(s) in All CE5xx/UC5xx.

Note The new created VLAN shown on the screen will be synchronized with VLANs on all other SBCS system that CCA 1.6 supports; such as in our case UC520. Under the hostname UC520 you can show that a new VLAN was created

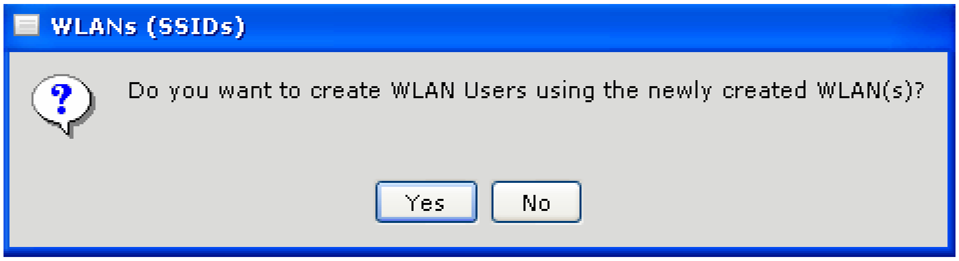


Hostname: UC520-demo

VLAN ID	VLAN Name
1	default
20	Guest
30	data-open
40	data-secure
50	vlan0050
60	Cisco-Guest
100	Cisco-Voice

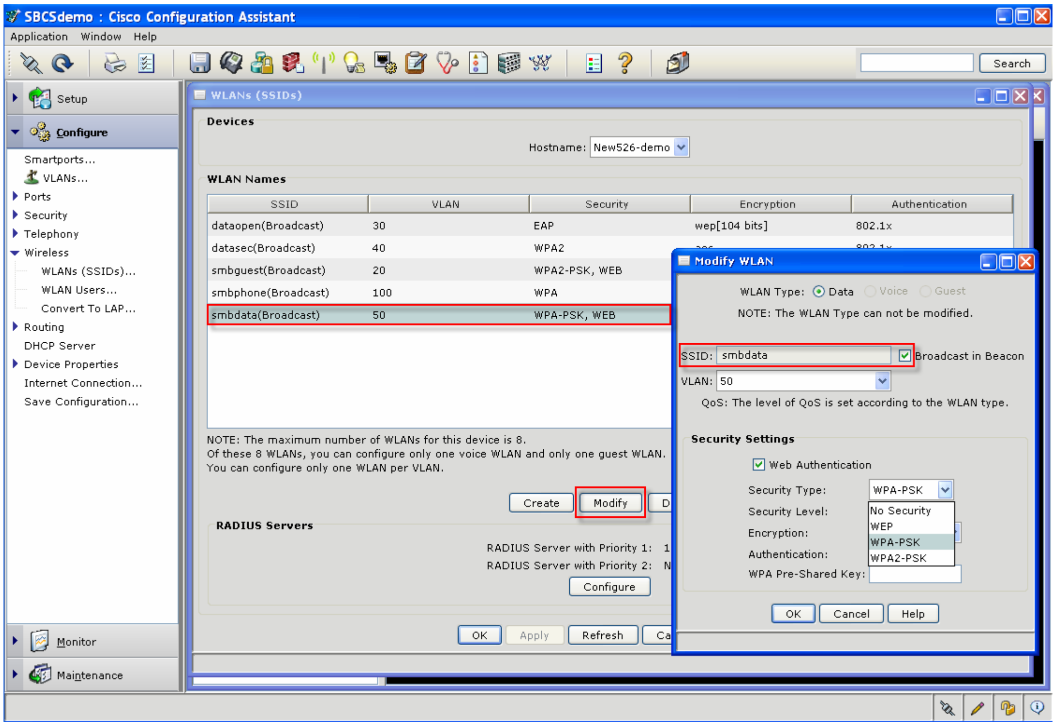
Total Rows: 7

If you are creating a SSID with WebAuth you will also get a message if a new WLAN user should be created at the same time. Also a new feature in the CCA 1.6



Do you want to create WLAN Users using the newly created WLAN(s)?

STEP 5. Under **Wireless >WLANs (SSID)…>Modify** you can modify the SSID setting such as Security, Encryption, Choose associated VLAN and decide whether the SSID should be broadcasted.



SBCSdemo : Cisco Configuration Assistant — WLANs (SSIDs)

Devices

Hostname: New526-demo

WLAN Names

SSID	VLAN	Security	Encryption	Authentication
dataopen(Broadcast)	30	EAP	wep[104 bits]	802.1x
datasec(Broadcast)	40	WPA2		
smbguest(Broadcast)	20	WPA2-PSK, WEB		
smbphone(Broadcast)	100	WPA		
smbdata(Broadcast)	50	WPA-PSK, WEB		

NOTE: The maximum number of WLANs for this device is 8.
Of these 8 WLANs, you can configure only one voice WLAN and only one guest WLAN.
You can configure only one WLAN per VLAN.

RADIUS Servers

RADIUS Server with Priority 1:
RADIUS Server with Priority 2:

Modify WLAN

WLAN Type: ● Data ○ Voice ○ Guest

NOTE: The WLAN Type can not be modified.

SSID: smbdata ☑ Broadcast in Beacon

VLAN: 50

QoS: The level of QoS is set according to the WLAN type.

Security Settings

☑ Web Authentication

Security Type: WPA-PSK

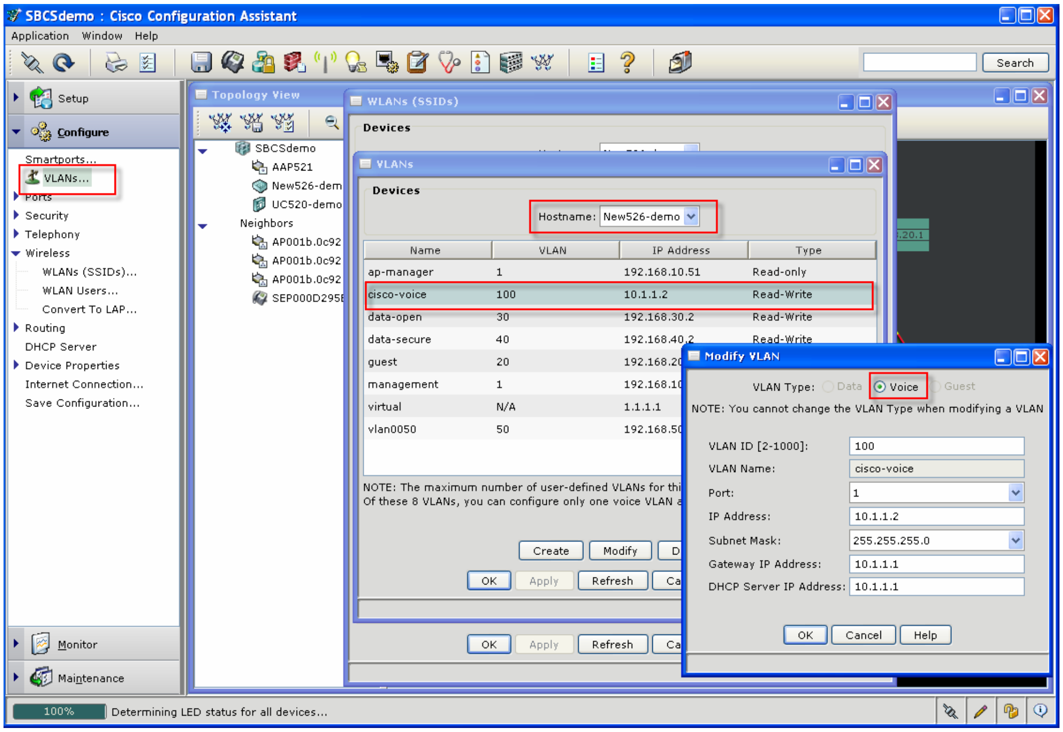
Security Level:

Encryption:

Authentication:

WPA Pre-Shared Key:

STEP 6. Under **<Configure> <VLANs…>** and then selecting < **New526-demo**> for the Hostname you can see all the dynamic interfaces (VLANs) that exist on your wireless network and their IP addresses assignments. We can see the same information under WebUI.



SBCSdemo : Cisco Configuration Assistant — VLANs

Devices

Hostname: New526-demo

Name	VLAN	IP Address	Type
ap-manager	1	192.168.10.51	Read-only
cisco-voice	100	10.1.1.2	Read-Write
data-open	30	192.168.30.2	Read-Write
data-secure	40	192.168.40.2	Read-Write
guest	20	192.168.20	
management	1	192.168.10	
virtual	N/A	1.1.1.1	
vlan0050	50	192.168.50	

NOTE: The maximum number of user-defined VLANs for thi
Of these 8 VLANs, you can configure only one voice VLAN a

Modify VLAN

VLAN Type: ○ Data ● Voice ○ Guest

NOTE: You cannot change the VLAN Type when modifying a VLAN

VLAN ID [2-1000]: 100

VLAN Name: cisco-voice

Port: 1

IP Address: 10.1.1.2

Subnet Mask: 255.255.255.0

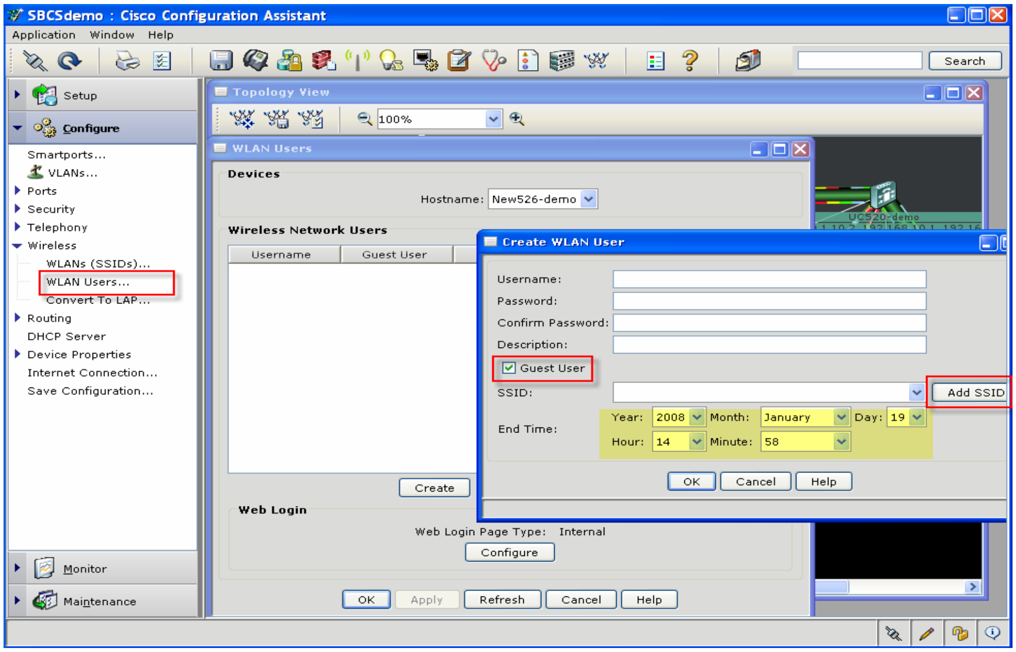
Gateway IP Address: 10.1.1.1

DHCP Server IP Address: 10.1.1.1

100% Determining LED status for all devices...

© 2008 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

STEP 7. Under **Wireless> WLAN Users>** you can create a new Wireless Network Users – a Regular User with no time restrictions or a Guest user with time restrictions.



Hostname: New526-demo

Create WLAN User

Username:

Password:

Confirm Password:

Description:

☑ Guest User

SSID:

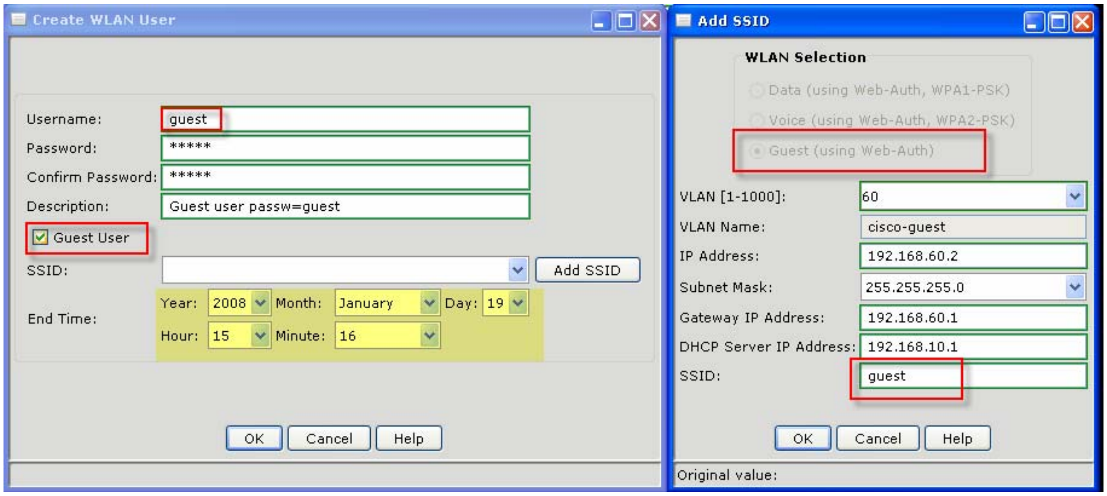
End Time: Year: 2008 Month: January Day: 19 Hour: 14 Minute: 58

Web Login Page Type: Internal

Note The new created Guest user option allows you to specify the Validity time of the Guest User on the network.

In addition you have an option to create a new SSID right from the same configuration screen. These are a new feature in the CCA 1.6 and new WLC software.

STEP 8. Under **WLAN Users** create a **guest** user; when you create a guest user you will have to add a **guest** SSID and create synchronized VLAN at the same time. For ease of use all this is done from one screen and the user gets prompted for each step during the process. All the newly created VLANs get synchronized across SBCS system for configuration simplicity.



Create WLAN User

Username: guest

Password: *****

Confirm Password: *****

Description: Guest user passw=guest

☑ Guest User

SSID:

End Time: Year: 2008 Month: January Day: 19 Hour: 15 Minute: 16

Add SSID

WLAN Selection

○ Data (using Web-Auth, WPA1-PSK)

○ Voice (using Web-Auth, WPA2-PSK)

● Guest (using Web-Auth)

VLAN [1-1000]: 60

VLAN Name: cisco-guest

IP Address: 192.168.60.2

Subnet Mask: 255.255.255.0

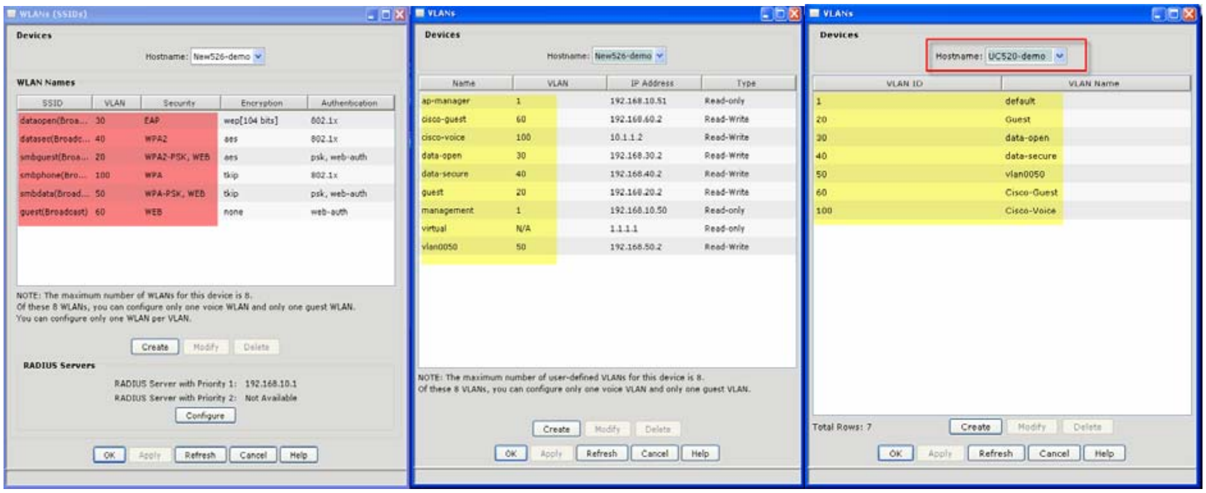
Gateway IP Address: 192.168.60.1

DHCP Server IP Address: 192.168.10.1

SSID: guest

Original value:

Note **When a new SSID gets created the system automatically sets the type of the WLAN to Guest from the three available options – Data, Voice, Guest. You can also demonstrate that the new SSIDs and VLANs were created successfully on the system as shown below.**



Hostname: New526-demo

SSID	VLAN	Security	Encryption	Authentication
dataopen(Broa...	30	EAP	wep[104 bits]	802.1x
datasec(Broadc...	40	WPA2	aes	802.1x
smbguest(Broa...	20	WPA2-PSK, WEB	aes	psk, web-auth
smbphone(Bro...	100	WPA	tkip	802.1x
smbdata(Broad...	50	WPA-PSK, WEB	tkip	psk, web-auth
guest(Broadcast)	60	WEB	none	web-auth

NOTE: The maximum number of WLANs for this device is 8.
Of these 8 WLANs, you can configure only one voice WLAN and only one guest WLAN.
You can configure only one WLAN per VLAN.

RADIUS Server with Priority 1: 192.168.10.1
RADIUS Server with Priority 2: Not Available

Hostname: New526-demo

Name	VLAN	IP Address	Type
ap-manager	1	192.168.10.51	Read-only
cisco-guest	60	192.168.60.2	Read-Write
cisco-voice	100	10.1.1.2	Read-Write
data-open	30	192.168.30.2	Read-Write
data-secure	40	192.168.40.2	Read-Write
guest	20	192.168.20.2	Read-Write
management	1	192.168.10.50	Read-only
virtual	N/A	1.1.1.1	Read-only
vlan0050	50	192.168.50.2	Read-Write

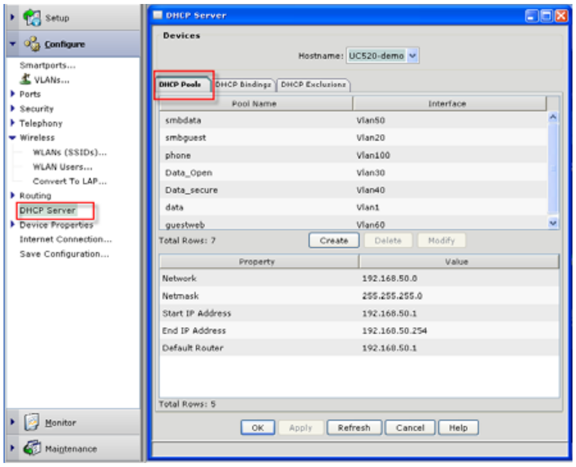
NOTE: The maximum number of user-defined VLANs for this device is 8.
Of these 8 VLANs, you can configure only one voice VLAN and only one guest VLAN.

Hostname: UC520-demo

VLAN ID	VLAN Name
1	default
20	Guest
30	data-open
40	data-secure
50	vlan0050
60	Cisco-Guest
100	Cisco-Voice

Total Rows: 7

STEP 9. DHCP services are not available on the Wireless controller so we will reserve to using the DHCP server on the UC500 to assign IP addresses to the wireless APs and wireless clients After the WLANs and VLANs have been created and configured verify or configure DHCP server on the UC500 in the <**Configure**><**Routing**> < **DHCP Server**> tab. Verify that DHCP Pools and DHCP Exclusions are created and configured properly on the UC520 for each VLAN previously configured.



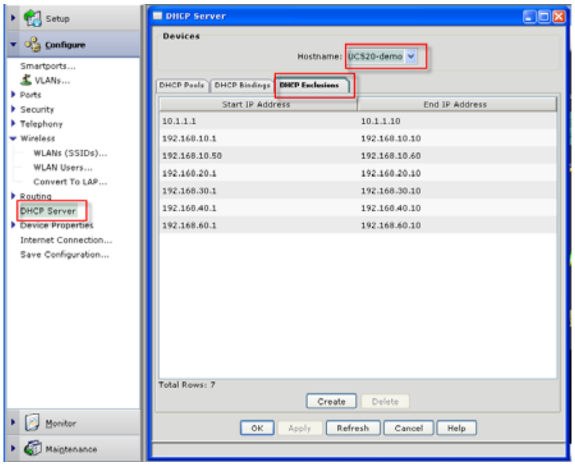
Hostname: UC520-demo

Pool Name	Interface
smbdata	Vlan50
smbguest	Vlan20
phone	Vlan100
Data_Open	Vlan30
Data_secure	Vlan40
data	Vlan1
guestweb	Vlan60

Total Rows: 7

Property	Value
Network	192.168.50.0
Netmask	255.255.255.0
Start IP Address	192.168.50.1
End IP Address	192.168.50.254
Default Router	192.168.50.1

Total Rows: 5

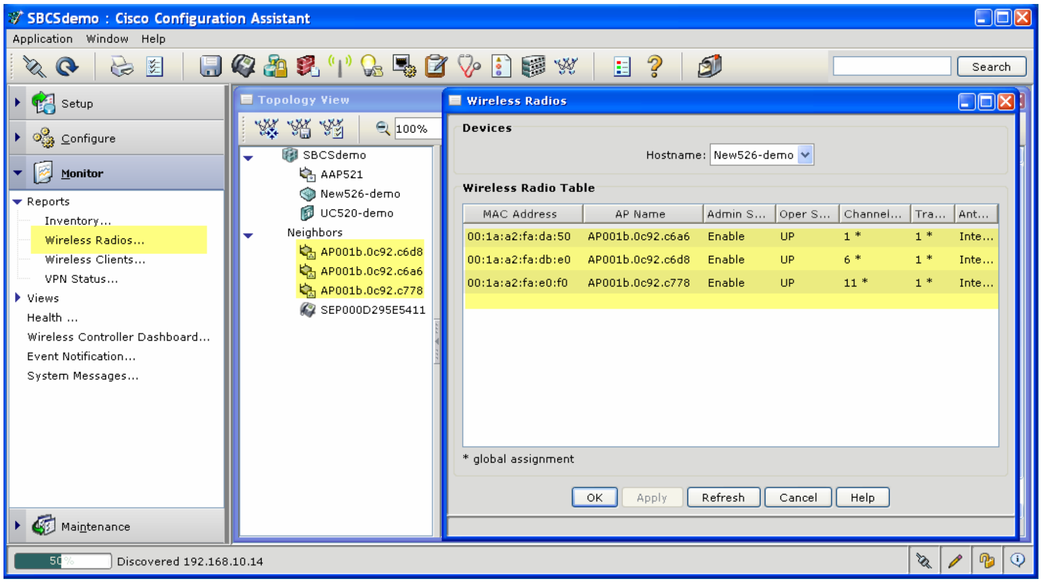


Hostname: UC520-demo

Start IP Address	End IP Address
10.1.1.1	10.1.1.10
192.168.10.1	192.168.10.10
192.168.10.50	192.168.10.60
192.168.20.1	192.168.20.10
192.168.30.1	192.168.30.10
192.168.40.1	192.168.40.10
192.168.60.1	192.168.60.10

Total Rows: 7

STEP 10. Next move on the **Monitor** Tab and see some of the options there. Under **Monitor>Reports** you can see all wireless Radios (APs) and wireless clients on the network.



Devices

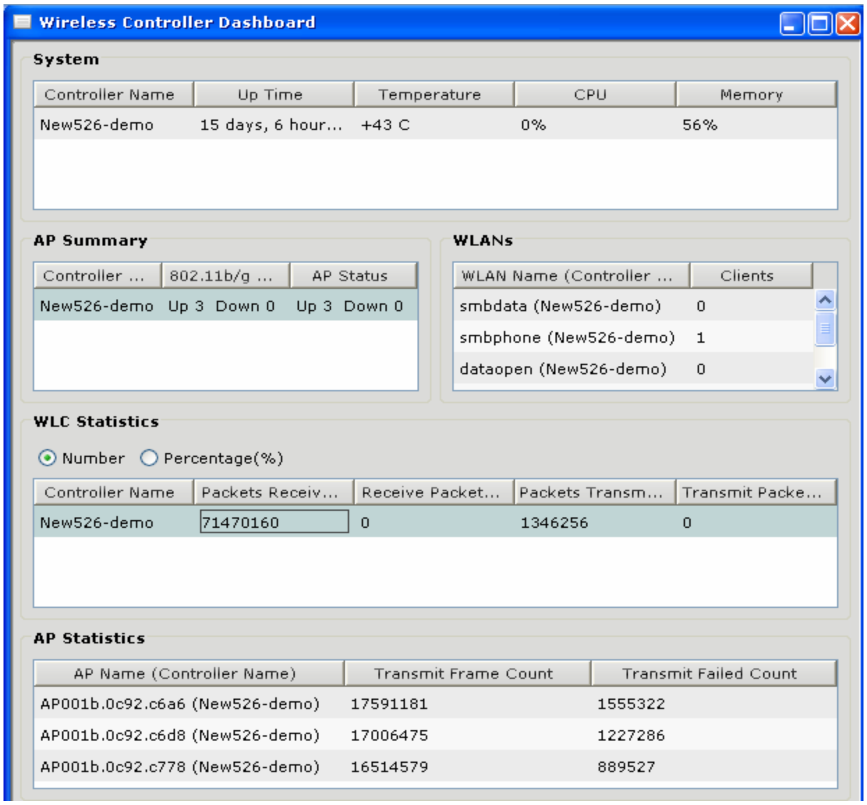
Hostname: New526-demo

Wireless Radio Table

MAC Address	AP Name	Admin S...	Oper S...	Channel...	Tra...	Ant...
00:1a:a2:fa:da:50	AP001b.0c92.c6a6	Enable	UP	1 *	1 *	Inte...
00:1a:a2:fa:db:e0	AP001b.0c92.c6d8	Enable	UP	6 *	1 *	Inte...
00:1a:a2:fa:e0:f0	AP001b.0c92.c778	Enable	UP	11 *	1 *	Inte...

* global assignment

STEP 11. Next lets take a look at the **Monitor>Wireless Controller Dashboard > tab** – this is also a new option in the CCA 1.6. Under this option you can show System Status, AP summary, Controller and AP Statistics



System

Controller Name	Up Time	Temperature	CPU	Memory
New526-demo	15 days, 6 hour...	+43 C	0%	56%

AP Summary

Controller ...	802.11b/g ...	AP Status
New526-demo	Up 3 Down 0	Up 3 Down 0

WLANs

WLAN Name (Controller ...	Clients
smbdata (New526-demo)	0
smbphone (New526-demo)	1
dataopen (New526-demo)	0

WLC Statistics

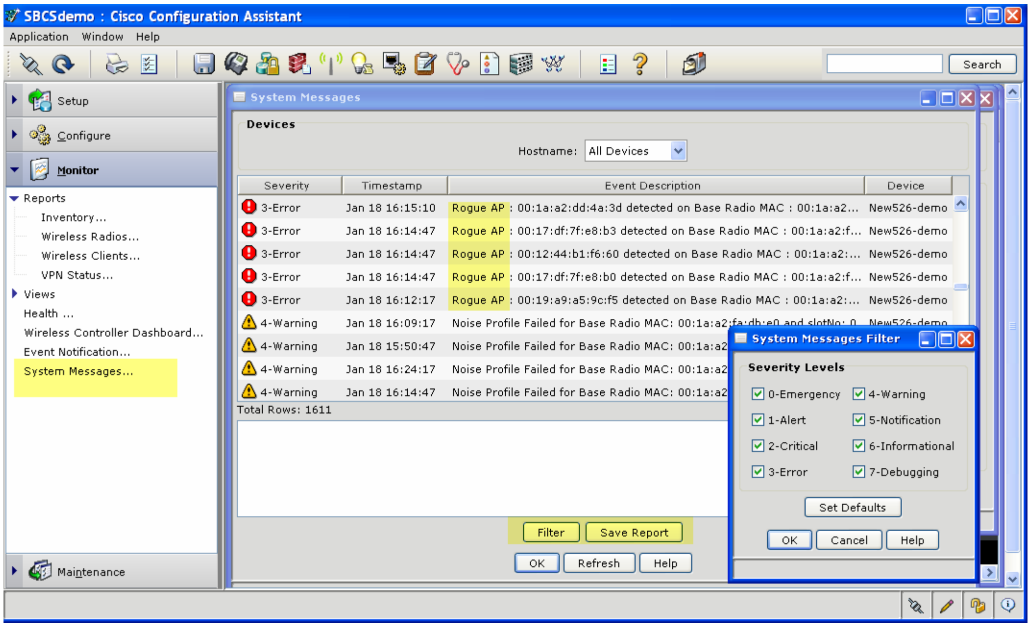
● Number ○ Percentage(%)

Controller Name	Packets Receiv...	Receive Packet...	Packets Transm...	Transmit Packe...
New526-demo	71470160	0	1346256	0

AP Statistics

AP Name (Controller Name)	Transmit Frame Count	Transmit Failed Count
AP001b.0c92.c6a6 (New526-demo)	17591181	1555322
AP001b.0c92.c6d8 (New526-demo)	17006475	1227286
AP001b.0c92.c778 (New526-demo)	16514579	889527

STEP 12. Next lets take a look at the **Monitor>System Messages** tab – if there are any rogues AP in the surrounding environment and not configured on you network the system will display them as Rogue APs. You may also setup a Message Filter or Save/Print the system messages report.



Devices

Hostname: All Devices

Severity	Timestamp	Event Description	Device
3-Error	Jan 18 16:15:10	Rogue AP : 00:1a:a2:dd:4a:3d detected on Base Radio MAC : 00:1a:a2...	New526-demo
3-Error	Jan 18 16:14:47	Rogue AP : 00:17:df:7f:e8:b3 detected on Base Radio MAC : 00:1a:a2:f...	New526-demo
3-Error	Jan 18 16:14:47	Rogue AP : 00:12:44:b1:f6:60 detected on Base Radio MAC : 00:1a:a2:...	New526-demo
3-Error	Jan 18 16:14:47	Rogue AP : 00:17:df:7f:e8:b0 detected on Base Radio MAC : 00:1a:a2:f...	New526-demo
3-Error	Jan 18 16:12:17	Rogue AP : 00:19:a9:a5:9c:f5 detected on Base Radio MAC : 00:1a:a2:...	New526-demo
4-Warning	Jan 18 16:09:17	Noise Profile Failed for Base Radio MAC: 00:1a:a2:fa:db:e0 and slotNo: 0	New526-demo
4-Warning	Jan 18 15:50:47	Noise Profile Failed for Base Radio MAC: 00:1a:a2	
4-Warning	Jan 18 16:24:17	Noise Profile Failed for Base Radio MAC: 00:1a:a2	
4-Warning	Jan 18 16:14:47	Noise Profile Failed for Base Radio MAC: 00:1a:a2	

Total Rows: 1611

Severity Levels

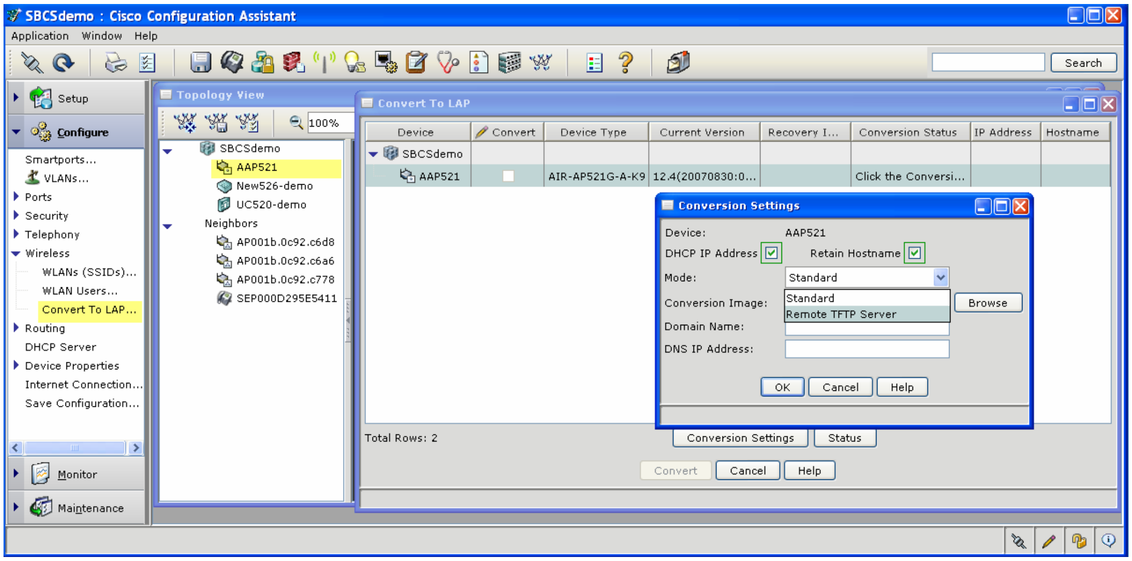
☑ 0-Emergency ☑ 4-Warning
☑ 1-Alert ☑ 5-Notification
☑ 2-Critical ☑ 6-Informational
☑ 3-Error ☑ 7-Debugging

Note The error messages displayed on the display will vary from site to site.

Converting 521 AP from Standalone to Controller mode LAP

STEP 13. Under **Configure>Wireless>Convert To LAP…>** you can convert any or all Standalone 521 APs to a Controller Mode LAPs. You can demonstrate that there is a standalone 521 AP connected to the SBCS demo network and that AP can be converted to the LAP.

Note **Do not proceed with the conversation process during the demonstration. In addition you will have to verify that the Standalone 521 AP is part of the SBCS-demo community, otherwise the <Convert To LAP…> will not show up under the <Wireless> menu option.**



Device	Convert	Device Type	Current Version	Recovery I...	Conversion Status	IP Address	Hostname
SBCSdemo							
AAP521	☐	AIR-AP521G-A-K9	12.4(20070830:0...		Click the Conversi...		

Conversion Settings

Device: AAP521

DHCP IP Address ☑ Retain Hostname ☑

Mode: Standard

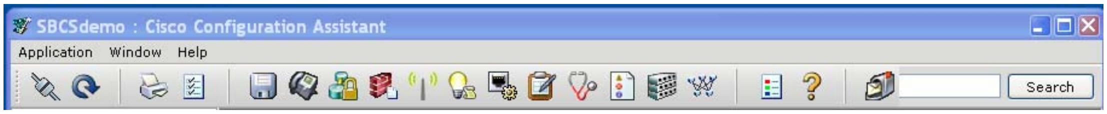
Conversion Image: Standard / Remote TFTP Server

Domain Name:

DNS IP Address:

Total Rows: 2

Viewing Horizontal Menu Tab in the CCA



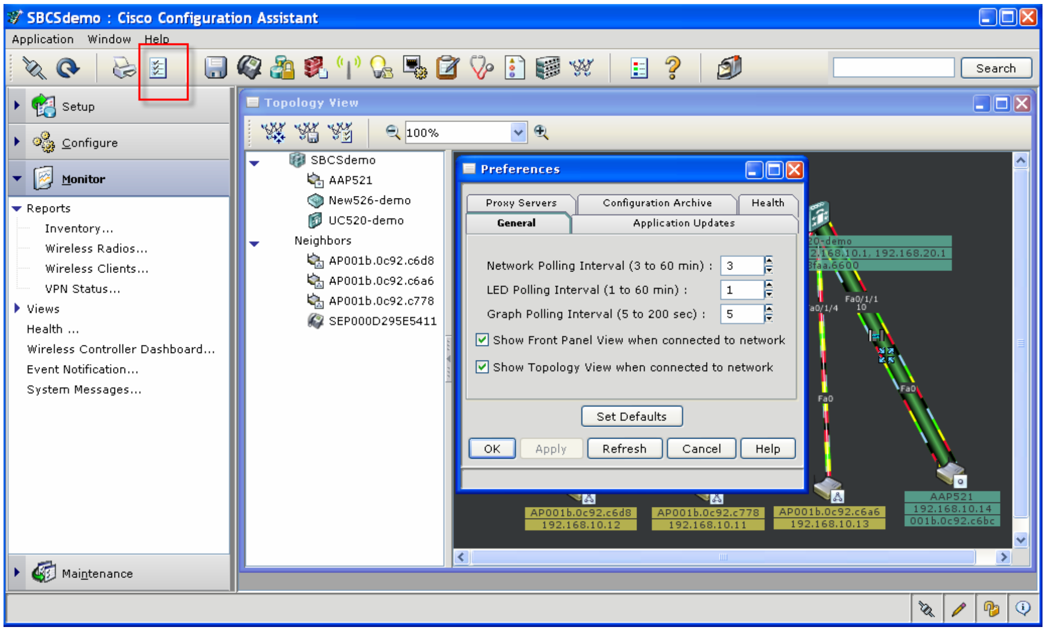
The Client filter further enable the ability to view specific information relating to client IP Address, MAC Address, Name, and asset information.

STEP 1. The First Tab allows to connect or change the community you are displaying

STEP 2. The second Tab is the refresh button, when you make changes and need to refresh the information presented on the screen or the Topology view.

STEP 3. The Third Tab activates the Print Services

STEP 4. The Forth Tab is the preference setting tab, here you can change setting such as Network Polling Intervals, setup Applications Updates, Proxy Servers, Configuration Archive and Network Health



Network Polling Interval (3 to 60 min) : 3

LED Polling Interval (1 to 60 min) : 1

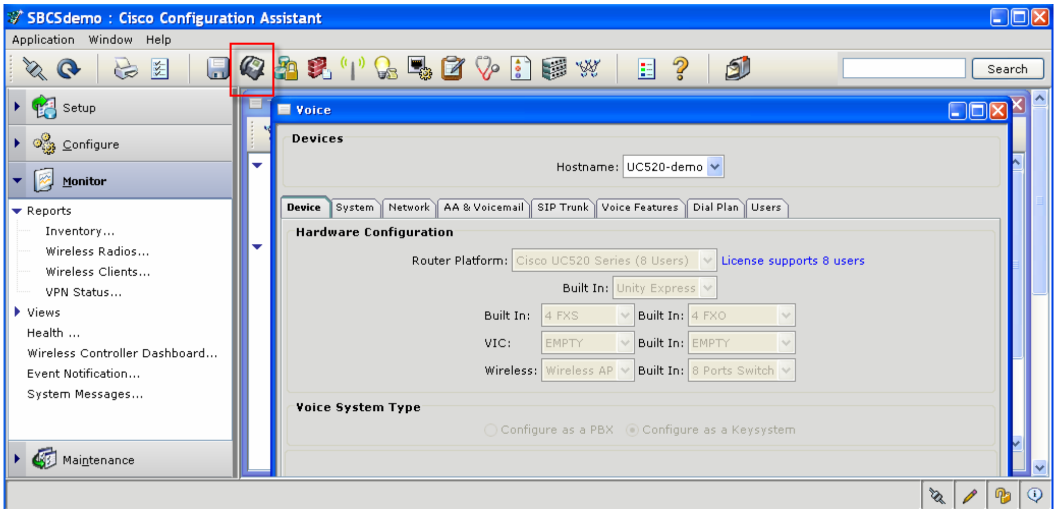
Graph Polling Interval (5 to 200 sec) : 5

☑ Show Front Panel View when connected to network

☑ Show Topology View when connected to network

STEP 5. Next Tab save configurations of all or individual devices

STEP 6. The allows you to configure Voice setting such as: Device and System Parameters, Network parameters, Dial Plan, AA and Voicemail, SIP trunk parameters, Voice Features and User Parameters.



Hostname: UC520-demo

Router Platform: Cisco UC520 Series (8 Users) License supports 8 users

Built In: Unity Express

Built In: 4 FXS Built In: 4 FXO

VIC: EMPTY Built In: EMPTY

Wireless: Wireless AP Built In: 8 Ports Switch

○ Configure as a PBX ● Configure as a Keysystem

STEP 7. The . tab is to Cofigure VPN server on the UC520

STEP 8. Next Tab is to setup Firewall and DMZ on the UC 520 and different Security Levels.

STEP 9. The Wireless Tab allows you to configure Wireless setting on the UC520 device for the Stand- alone AP(s) and on the WLC 526 for the Controller Mode configuration.

Note This setting is the same as if you would choose a Wireless Networks Configuration on the left side Config Wireless Tab. Several other Tabs on the Horizontal Menu are a repeat of the configuration options available on the Left Side Menu options.

STEP 10. Next Tab is the setting to configure the Smart Ethernet ports on the UC 520 or CE 500 if one is available.

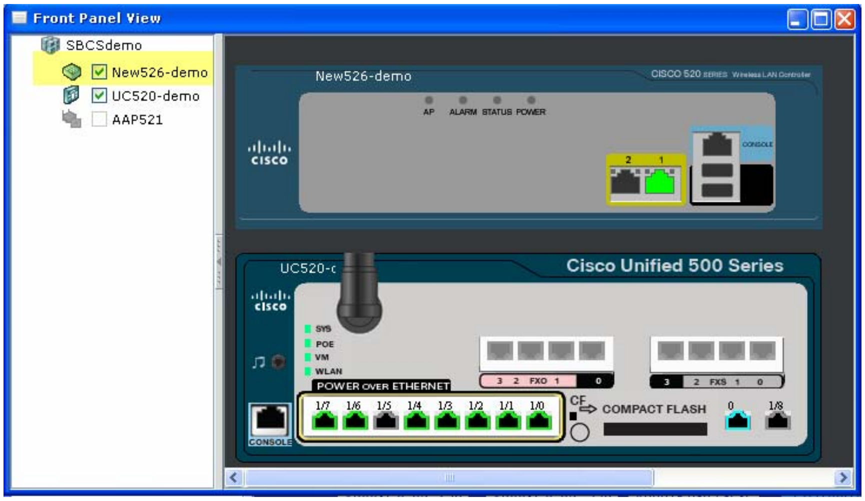
STEP 11. The next Tab is the Ethernet Port Setting tab on the UC 520 with options to set filters on each port and set the speed of the ports.

STEP 12. The tab is the Inventory Tab , it provides a detailed list of the devices and their settings.

STEP 13. The next tab is the Health Tab, same as the Monitor tab on the laft side menu and shows the performance of the system.

STEP 14. The Tab is the event notification tab, also same as Monitor Health Tab on the left side menu.

STEP 15. Next Tab is the Front View Menu Tab of the devices in the SBCS network.



Note The Front View of the WLC 526 is now supported in release version 1.6 of the CCA

STEP 16. The next Tab displays and refreshes the Network Topology View on the screen.

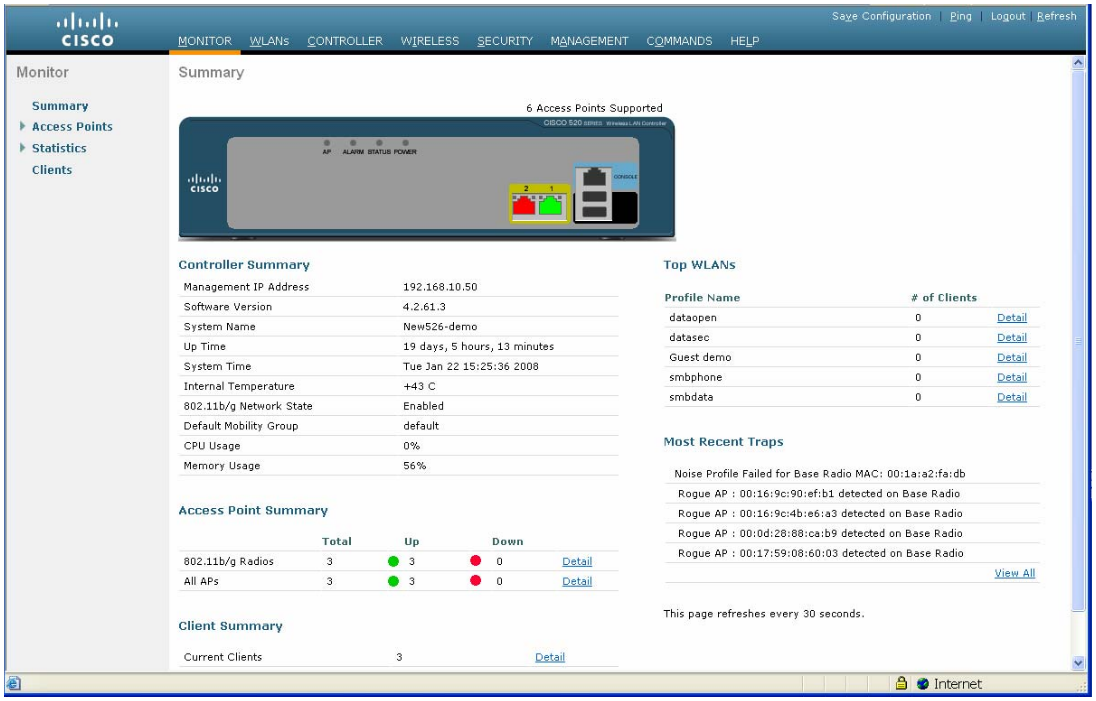
STEP 17. And the next four Tabs Search are for Legend, Help, Email option and Search.

Configuring 526 Wireless LAN Controllers

STEP 1. There are Unified Controllers and SMB controllers, you want to briefly discuss the differences between the Unified and Mobility Express 526 controller

STEP 2. The Cisco controllers provide Mobility Express management for SMB system

STEP 3. If desired, you can show demonstrate the web interface of the 526 controller or the CCA interface to the Controller. You can lunch CCA from the desktop Icon as before or lunch the WebUI to the controller by lunching the IE browser to the http://192.168.10.50 - the IP address of the management interface of the 526 controller.



Summary

6 Access Points Supported

Controller Summary

Management IP Address	192.168.10.50
Software Version	4.2.61.3
System Name	New526-demo
Up Time	19 days, 5 hours, 13 minutes
System Time	Tue Jan 22 15:25:36 2008
Internal Temperature	+43 C
802.11b/g Network State	Enabled
Default Mobility Group	default
CPU Usage	0%
Memory Usage	56%

Access Point Summary

	Total	Up	Down	
802.11b/g Radios	3	● 3	● 0	Detail
All APs	3	● 3	● 0	Detail

Client Summary

Current Clients	3	Detail

Top WLANs

Profile Name	# of Clients	
dataopen	0	Detail
datasec	0	Detail
Guest demo	0	Detail
smbphone	0	Detail
smbdata	0	Detail

Most Recent Traps

Noise Profile Failed for Base Radio MAC: 00:1a:a2:fa:db
Rogue AP : 00:16:9c:90:ef:b1 detected on Base Radio
Rogue AP : 00:16:9c:4b:e6:a3 detected on Base Radio
Rogue AP : 00:0d:28:88:ca:b9 detected on Base Radio
Rogue AP : 00:17:59:08:60:03 detected on Base Radio
View All

This page refreshes every 30 seconds.

Auto Radio Frequency (RF) and Power Management

In this section, you can demo auto power and auto channel assignments. The Auto RF demos rely on the controller response time which is locked in at 600 seconds (10 minutes). Patience is required for some of the RF changes to occur.

Auto Power and DCA

STEP 1. For this demonstration use Web UI interface on the controller. Connect to the controller Web UI interface IP address 192.168.10.50 (in our case the IP address of the controller management interface). Login into the controller with username = admin and password = cisco

STEP 2. In the controller GUI interface go to **wireless>802.11b/g > RRM >auto RF** and you will see all the default options. These options are preset and should not be changed.

STEP 3. In the controller GUI interface go to **wireless>802.11b/g > RRM >DCA** you can see all the channels that have been selected**.** There are three channels selected 1, 6, 11 – these are the non-overlapping channels do not change that setting.

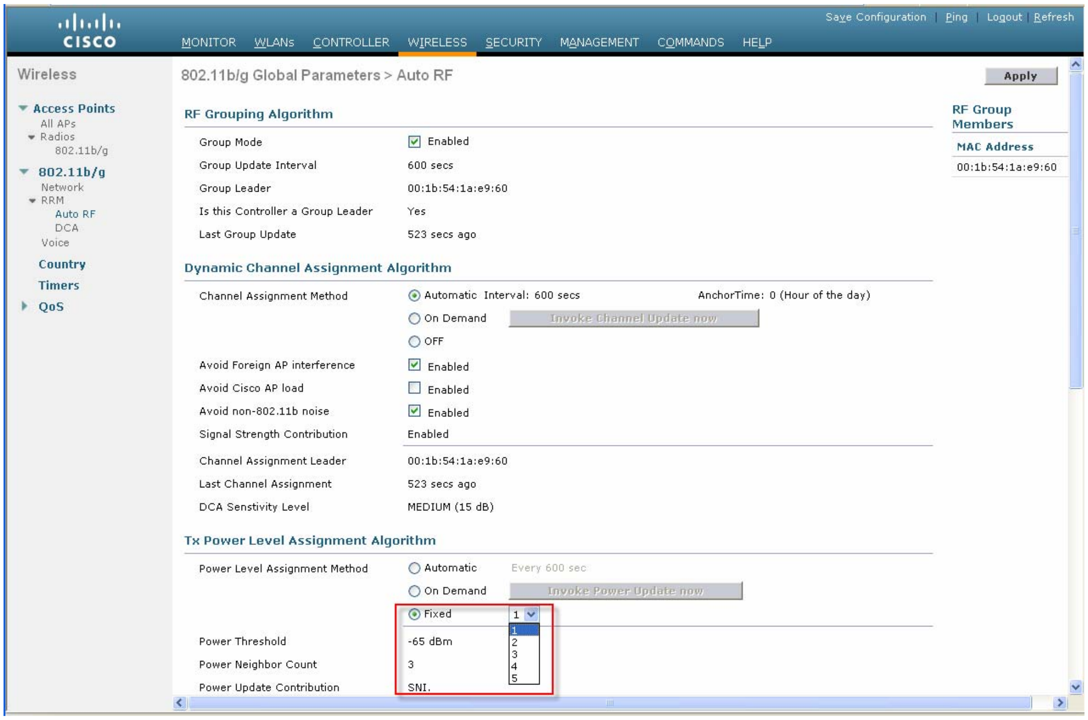
STEP 4. In the section you can also choose the country of operation – please select the desired country here under the **802.11 b/g > Country setting.**

Note The APs should be setup in a six foot by six foot grid with the WLC526 in the center of the grid. For the best demonstration results 3 to 4 LAPs 521 should be used. For RRM to function effectively at least 3 LAP 521 should be used at the same time.

STEP 5. Disconnect one of the APs from the Ethernet ports

STEP 6. Look in the CCA under **Monitor>Wireless Radios** some of the transmit power settings should change from the lowest value of 1*

STEP 7. The radio settings can be also observed under the Web UI under the **Wireless>Radios>802.12b/g > Tx Power Level Assignment in Custom Mode.**



802.11b/g Global Parameters > Auto RF

RF Grouping Algorithm

Group Mode ☑ Enabled
Group Update Interval 600 secs
Group Leader 00:1b:54:1a:e9:60
Is this Controller a Group Leader Yes
Last Group Update 523 secs ago

RF Group Members

MAC Address
00:1b:54:1a:e9:60

Dynamic Channel Assignment Algorithm

Channel Assignment Method ● Automatic Interval: 600 secs AnchorTime: 0 (Hour of the day)
○ On Demand
○ OFF
Avoid Foreign AP interference ☑ Enabled
Avoid Cisco AP load ☐ Enabled
Avoid non-802.11b noise ☑ Enabled
Signal Strength Contribution Enabled
Channel Assignment Leader 00:1b:54:1a:e9:60
Last Channel Assignment 523 secs ago
DCA Senstivity Level MEDIUM (15 dB)

Tx Power Level Assignment Algorithm

Power Level Assignment Method ○ Automatic Every 600 sec
○ On Demand
● Fixed 1
1
2
3
4
5
Power Threshold -65 dBm
Power Neighbor Count 3
Power Update Contribution SNI.

Note:

Power Level	The transmit power level of the access point where 1 = Maximum power allowed per Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 6.25 to 12.5% power, and 5 = 0.195 to 6.25% power **Note** The power levels and available channels are defined by the Country Code setting, and are regulated on a country by country basis.

STEP 8. Connect AP back to the Ethernet port and you should be able to observer changes in Power Levels.

Note This demonstration works the best if at least 3 APs are being used.

Emphasize:

- The real-time RF management capabilities of the Cisco Mobility Express Wireless Network allow the network to respond in real-time to changes in the RF environment.

1 Organization should expect ongoing changes in the RF environment.

2 Users come and go from conference rooms.

3 Additional clients may be added to an area in a building

4 The WLAN infrastructure may need to be adjusted over time for changes in the building configuration or design.

5 Interference can occur from devices operating in the unlicensed Wi-Fi bands

- The Cisco Mobility Express Wireless Network creates an intelligent RF control plane for self-configuration, self-healing, and self-optimization.
- Intelligent RF capabilities managed by Cisco wireless LAN controllers include:

6 Dynamic Channel Assignment---802.11 channels are adjusted to optimize network coverage and performance based on changing RF conditions.

7 Interference Detection and Avoidance---The system detects interference and recalibrates the network to avoid performance problems.

8 Coverage Hole Detection and Correction---RRM software detects coverage holes and attempts to correct them by adjusting the power output of access points.

9 Dynamic power control---The system dynamically adjusts the power output of individual access points to accommodate changing network conditions, helping to ensure predictable wireless performance and availability

MOBILITY EXPRESS SECURITY AND GUEST ACCESS

Demo Time: 10 to 20 minutes

Customers understand the need for wireless security. At issue is how to manage the security across the enterprise given today's access requirements for employees and guest access. Other critical issues facing customers include Rogue APs . The demonstrations included in this section are shown in Table 5.

Table 5. Security Setup Demos

Demo	Duration (min.)	Description
Guest Access using Web Authentication (configuration demo)	5 - 10	This demo will show a customer how to setup a Guest authentication web login.
WEB Authentication	5	This demo will show how to monitor guest login

Key Features

- Multiple security policies are very easy to deploy and maintain across any network using Cisco Mobility Express WLAN Solution.
- Built in guest user administration web authentication is a key feature many customers require for guest access.

Marketing Messages

With the increased reliance on WLANs, businesses are becoming more concerned about network security. Network managers need to provide end users with freedom and mobility without offering intruders' access to the WLAN or the information sent and received on the wireless network.

The Cisco Mobility Express Wireless solution provides robust wireless LAN security services that closely parallel the security available in a wired LAN. It fulfills the need for consistent, reliable, and secure mobile networking by delivering industry-leading WLAN security services. The Cisco Mobility Express Wireless solution delivers many innovative Cisco enhancements and supports Wi-Fi Protected Access (WPA), Wi-Fi Protected Access 2 (WPA2), and Wi-Fi Certified client devices to provide access control via per-user, per-session mutual authentication and data privacy via strong dynamic encryption.

Demonstration Notes

Demo Actions

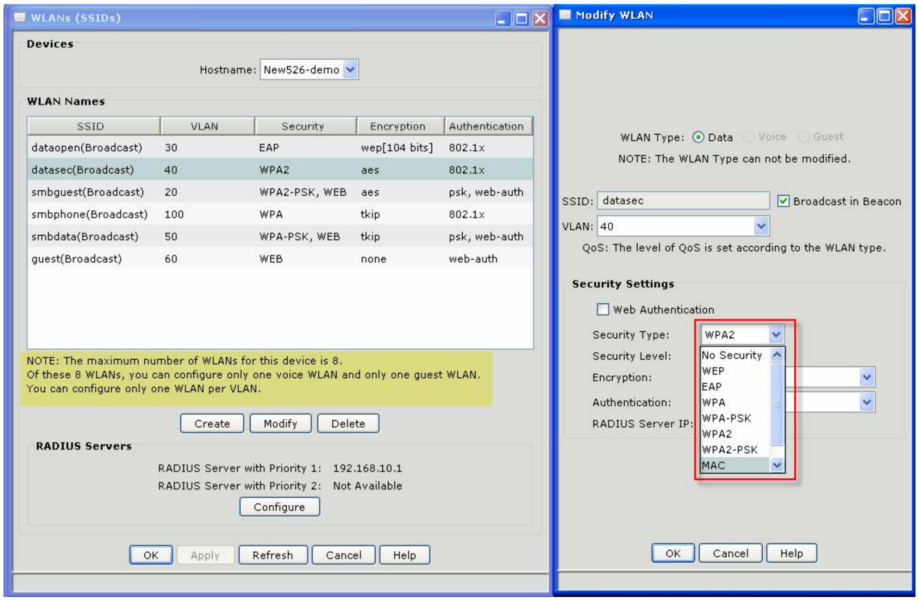
Mobility Express Security Configuration

STEP 1. In the CCA 1.6 go to **Configure>Wireless> WLANs (SSIDs)…>** and choose the **Hostname** to be configured

STEP 2. In this section you notice that each SSID is mapped to a VLAN –

Note: only one to one mapping is allowed; one SSID per VLAN

STEP 3. Choose one of the SSIDs configured in earlier and then click **Modify. For example choose <datasec>**



Hostname: New526-demo

SSID	VLAN	Security	Encryption	Authentication
dataopen(Broadcast)	30	EAP	wep[104 bits]	802.1x
datasec(Broadcast)	40	WPA2	aes	802.1x
smbguest(Broadcast)	20	WPA2-PSK, WEB	aes	psk, web-auth
smbphone(Broadcast)	100	WPA	tkip	802.1x
smbdata(Broadcast)	50	WPA-PSK, WEB	tkip	psk, web-auth
guest(Broadcast)	60	WEB	none	web-auth

NOTE: The maximum number of WLANs for this device is 8.
Of these 8 WLANs, you can configure only one voice WLAN and only one guest WLAN.
You can configure only one WLAN per VLAN.

RADIUS Server with Priority 1: 192.168.10.1
RADIUS Server with Priority 2: Not Available

WLAN Type: ● Data ○ Voice ○ Guest
NOTE: The WLAN Type can not be modified.

SSID: datasec ☑ Broadcast in Beacon
VLAN: 40
QoS: The level of QoS is set according to the WLAN type.

☐ Web Authentication
Security Type: WPA2
Security Level:
Encryption:
Authentication:
RADIUS Server IP:

No Security
WEP
EAP
WPA
WPA-PSK
WPA2
WPA2-PSK
MAC

STEP 4. Under the security settings you will see all of the security options available for configuration. In our case the **SSID = datasec** is configured with **WPA2** as a security option.

STEP 5. The encryption type for the SSID was chosen as "AES" the second option available is TKIP.

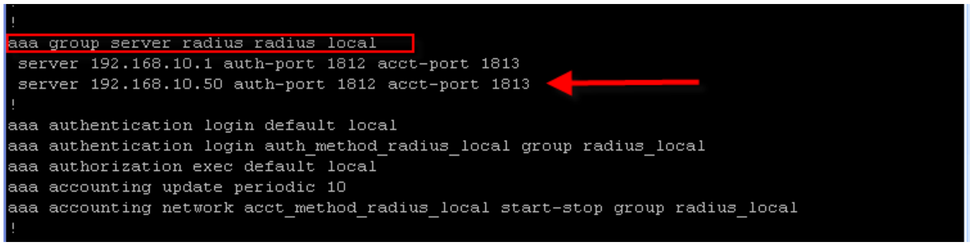
STEP 6. And finally the RADIUS server with IP address 192.168.10.1 was selected for 802.1x authentication as shown in the screen below

STEP 7. The RADIUS server can be selected as internal on the UC500 or external if External RADIUS such as ACS is available.

Note The Local RADIUS server on the UC520 is designed for support of the Internal or Standalone APs only!

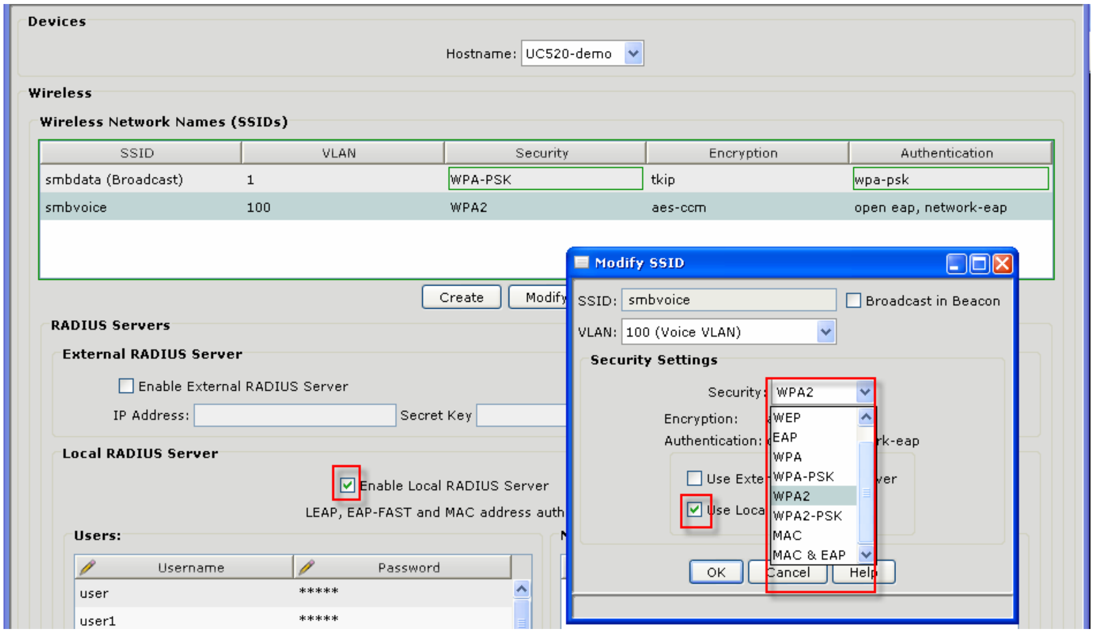
For the demonstration purposes only, we have to modify the UC520 local RADIUS server to also support WLC 526 as authenticator, therefore we need to add the following command on the UC520 from the CLI. The IP address added 192.168.50.10 indicates the IP address of the controller's management interface.

In the production environment do not use the UC520 as a RADIUS server for the 526 Wireless Controllers.



```
!
aaa group server radius radius_local
 server 192.168.10.1 auth-port 1812 acct-port 1813
 server 192.168.10.50 auth-port 1812 acct-port 1813
!
aaa authentication login default local
aaa authentication login auth_method_radius_local group radius_local
aaa authorization exec default local
aaa accounting update periodic 10
aaa accounting network acct_method_radius_local start-stop group radius_local
!
```

STEP 8. In our demonstration we have configured the internal Local RADIUS server on the UC 520 under **Configure>Wireless > WLANs > Hostname = UC520-demo. Secret Key = demo. Enable** Local RADIUS server.



Devices

Hostname: UC520-demo

Wireless

Wireless Network Names (SSIDs)

SSID	VLAN	Security	Encryption	Authentication
smbdata (Broadcast)	1	WPA-PSK	tkip	wpa-psk
smbvoice	100	WPA2	aes-ccm	open eap, network-eap

RADIUS Servers

External RADIUS Server

☐ Enable External RADIUS Server

IP Address: Secret Key

Local RADIUS Server

☑ Enable Local RADIUS Server

LEAP, EAP-FAST and MAC address auth

Users:

Username	Password
user	*****
user1	*****

Modify SSID

SSID: smbvoice ☐ Broadcast in Beacon

VLAN: 100 (Voice VLAN)

Security Settings

Security: WPA2

Encryption:

Authentication: rk-eap

☐ Use Exte ver

☑ Use Loca

STEP 9. Enable the “Local RADIUS Server” with “Secret Key = **demo**

STEP 10. Show client connectivity on the **SSID = smbdata**, with **username=user1 and password= demo**.

Note The supported EAP types with the Local RADIUS serer are LEAP; EAP-FAST and MAC authentication

Cisco Wireless Clients

Demo Time: 20 to 30 minutes

There are variety of the Wireless Client 802.11a/b/g cards are available on the market today. There are also about half a dozen very popular Supplicants available to the wireless users. Although we cannot demonstrate every possible wireless client and supplicant we will demonstrate the most popular clients, supplicants and some hand held devices used by the SMB. Please note the Wireless Clients demonstrated here are all CCX client devices.

The components highlighted in this demo section are shown in Table 6.

Table 6. Key Components to demonstrate various Client

Demo	Description
Laptop with CB 21AG card and Cisco ADU	Wireless client setup with the Cisco PC Bus 802.11 a/g card and Cisco ADU supplicant
Laptop with 350 card and ACU supplicant	Wireless client setup with Cisco 350 802.11b card and ACU
Laptop with CB 21AG card and ADU and CSSC 5.0 Supplicants	Wireless Client setup with Cisco card and Cisco Security Services Client Version 5.0
Intermec Hand Held Device and Funk Odyssey Supplicant (optional)	Intermec CN-3 Mobil device with Broadcoam Wireless Card and Funk Odyssey client
Cisco 7921 Wireless Phone	Cisco 7921 Wireless IP phone with VoIP
Nokia Dual Mode Phone (optional)	Nokia Dual Mode Wireless Phone.

Marketing Messages

Based on customer client requirements, you may want to discuss the various wireless client options available from Cisco (802.11b/g cards) or from 3rd party (Cisco Compatible –CCX) vendors. Over 90% of Wi-Fi silicon is Cisco Compatible

Cisco Compatible

Key Points:

- Using Cisco Client Administration Software, an administrator can centrally perform the following operations, thus minimizing cost to implement, operate, and optimize the wireless clients:
    - Determine and configure the setup options for the end user utility software
    - Set and modify end user functions
    - Create preconfigured user profiles for a user or group of users

For more info:

http://www.cisco.com/en/US/products/hw/wireless/ps4555/prod_maintenance_guides_list.html

Demo Activity

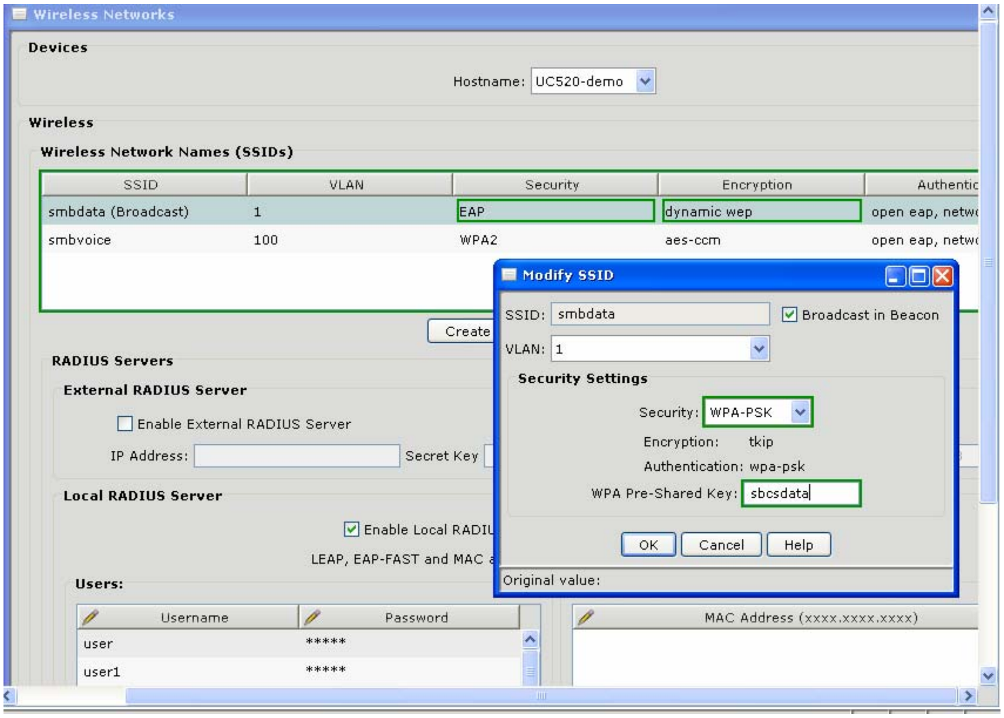
In this demonstration we will use variety of wireless cards and supplicants and to make demo more interesting and to explore rich set of the security capabilities of the Mobility Express controller in combination with the UC 520 we will demonstrate several different security setups (as shown in the previous section) with different clients. This demonstration will further enforce the security capabilities of the SMB system and its interoperability with a wide variety of wireless clients and supplicants. During the demonstration you may pass the wireless clients and handhelds to the customers.

Demo	Demo Duration	Demo Description
Laptop with CB 21AG card and Cisco ADU	3 min	Wireless client setup with the Cisco PC Bus 802.11 a/g card and Cisco ADU supplicant . **Demonstrate connectivity to WLC LAP with WPA2/AES and EAP-FAST**
Laptop with 350 card and ACU supplicant	3 min	Wireless client setup with Cisco 350 802.11b card and ACU **Demonstrate connectivity to IOS AP with EAP-FAST and Dynamic WEP**
Laptop with CB 21AG card CSSC 4.2 Supplicants	3 min	Wireless Client setup with Cisco card and Cisco Security Services Client Version 4.2 **Demonstrate connectivity to IOS AP with LEAP and Dynamic WEP.**
Laptop with Cisco CB 21AG card and CSSC 5.0 Supplicant	3min	Wireless Client setup with Cisco card and Cisco Security Services Client Version 5.0. **Demonstrate connectivity with WPA/PSK.**
Intermec Hand Held Device with Funk Odyssey Supplicant and MS Zero Config	3 min	Intermec CN-3 Mobil device with Broadcoam Wireless Card and Funk Odyssey client **Demonstrate connectivity with WPA-PSK using Zero Config and WPA2/AES and EAP-FAST using Odyssey supplicant**
Cisco 7921 Wireless Phone	3 min	Cisco 7921 Wireless IP phone with VoIP
Nokia Dual Mode Phone	3 min	Nokia Dual Mode Wireless Phone.

Wireless Client connectivity with UC520 integrated AP - Secure connectivity using CSSC supplicants.

We will demonstrate setup with WPA-PSK on the laptop using lately released CSSC version 5.0

STEP 1. Using CCA 1.6, in the Configure Wireless Networks tab configure **SSID=smbdata** with security WPA-PSK and **PSK=sbcsdata** or 1234567890; PSK key has to be at least 8 characters long.



Wireless Networks

Devices

Hostname: UC520-demo

Wireless

Wireless Network Names (SSIDs)

SSID	VLAN	Security	Encryption	Authentic
smbdata (Broadcast)	1	EAP	dynamic wep	open eap, netw
smbvoice	100	WPA2	aes-ccm	open eap, netw

Modify SSID

SSID: smbdata ☑ Broadcast in Beacon

VLAN: 1

Security Settings

Security: WPA-PSK

Encryption: tkip

Authentication: wpa-psk

WPA Pre-Shared Key: sbcsdata

Original value:

RADIUS Servers

External RADIUS Server

☐ Enable External RADIUS Server

IP Address: Secret Key

Local RADIUS Server

☑ Enable Local RADIU

LEAP, EAP-FAST and MAC a

Users:

Username	Password
user	*****
user1	*****

MAC Address (xxxx.xxxx.xxxx)

Note We are demonstrating connectivity with an autonomous AP on the UC 500

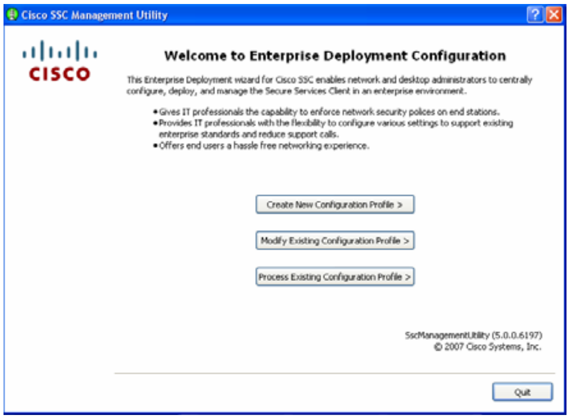
Note There are many Client Supplicants available and any of them should work with the Cisco Wireless System

Client connectivity demonstration using CSSC ver 5.0 supplicant

In this section we will demonstrate configuration and setting of the CSSC supplicant ver 5.0 with WPA-PSK and TKIP encryption. As shown in the step 2 other Authentication and Encryption options can be easily configured using CSSC ver 5.0 supplicant.

CSSC 5.X supports both Wired and Wireless connectivity on the client devices, however only one option by default is being used.

STEP 1. First we have to configure a profile using Configuration Manager 5.0

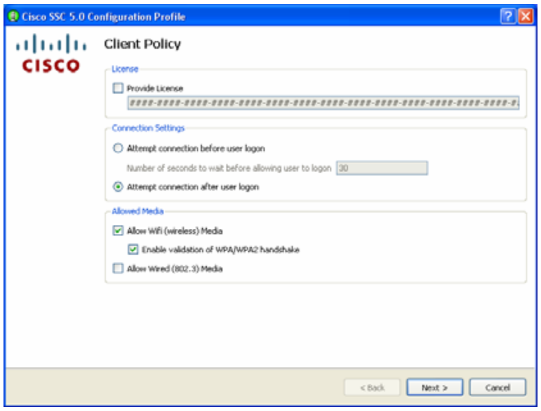

Cisco SSC Management Utility
Create New Configuration Profile >
Modify Existing Configuration Profile >
Process Existing Configuration Profile >
Quit

Welcome to Enterprise Deployment Configuration

This Enterprise Deployment wizard for Cisco SSC enables network and desktop administrators to centrally configure, deploy, and manage the Secure Services Client in an enterprise environment.

- Gives IT professionals the capability to enforce network security polices on end stations.
- Provides IT professionals with the flexibility to configure various settings to support existing enterprise standards and reduce support calls.
- Offers end users a hassle free networking experience.

SscManagementUtility (5.0.0.6197)
© 2007 Cisco Systems, Inc.



Client Policy

License

- □ Provide License
- ####-####-####-####-####-####-####-####-####-####-####-####-####-####-#

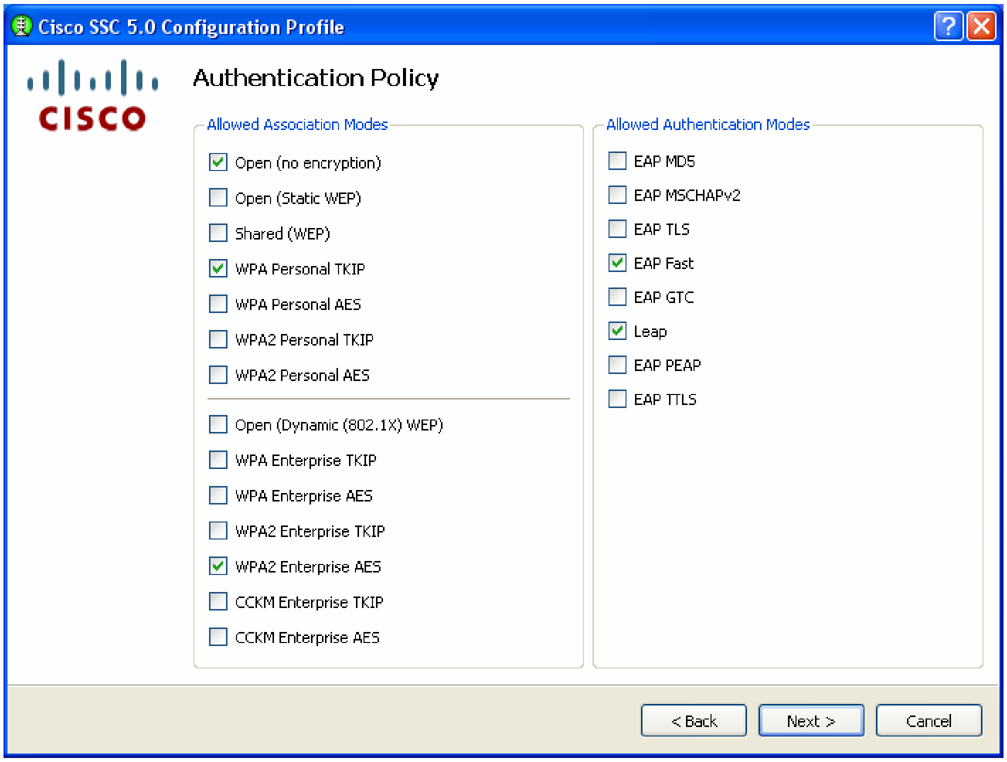
Connection Settings

- ○ Attempt connection before user logon
- Number of seconds to wait before allowing user to logon: 30
- ● Attempt connection after user logon

Allowed Media

- ☑ Allow Wifi (wireless) Media
- ☑ Enable validation of WPA/WPA2 handshake
- □ Allow Wired (802.3) Media

STEP 2. Enable Authentication Policy in the Supplicant for all the profiles of the wireless client. For our profile we have to make sure that WPA-PSK Personal with TKIP is enabled.



Authentication Policy

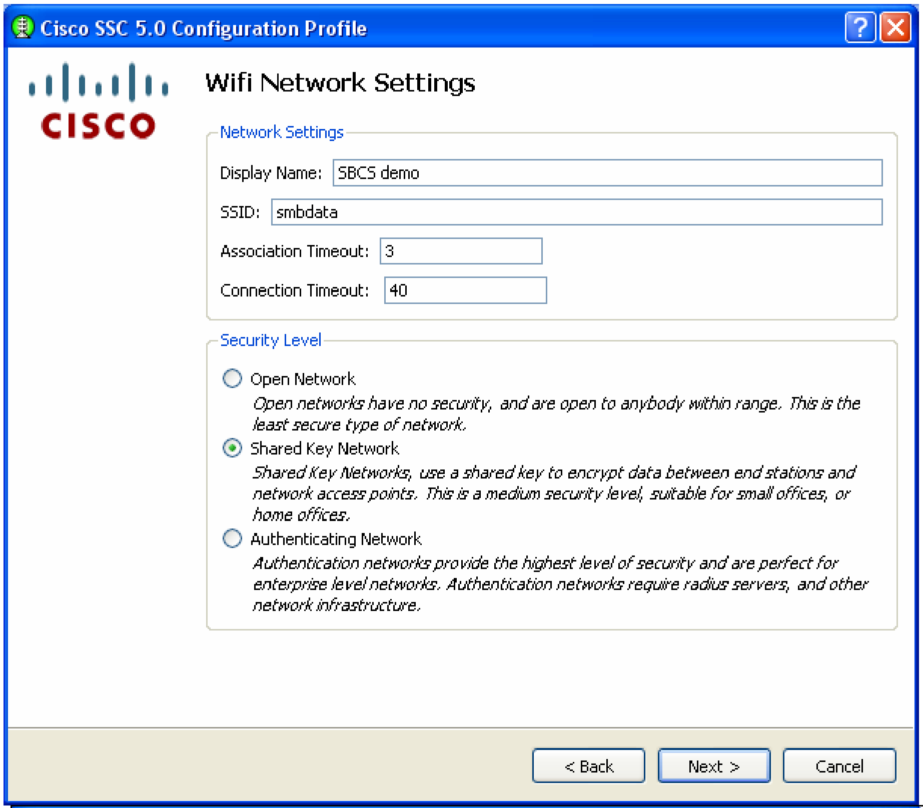
Allowed Association Modes

- ☑ Open (no encryption)
- □ Open (Static WEP)
- □ Shared (WEP)
- ☑ WPA Personal TKIP
- □ WPA Personal AES
- □ WPA2 Personal TKIP
- □ WPA2 Personal AES
- □ Open (Dynamic (802.1X) WEP)
- □ WPA Enterprise TKIP
- □ WPA Enterprise AES
- □ WPA2 Enterprise TKIP
- ☑ WPA2 Enterprise AES
- □ CCKM Enterprise TKIP
- □ CCKM Enterprise AES

Allowed Authentication Modes

- □ EAP MD5
- □ EAP MSCHAPv2
- □ EAP TLS
- ☑ EAP Fast
- □ EAP GTC
- ☑ Leap
- □ EAP PEAP
- □ EAP TTLS

STEP 3. In the next step we have to configure Wireless Settings for the client with **SSID=smbdata and shared key=sbcsdemo**



Wifi Network Settings

Network Settings

Display Name: SBCS demo

SSID: smbdata

Association Timeout: 3

Connection Timeout: 40

Security Level

○ Open Network

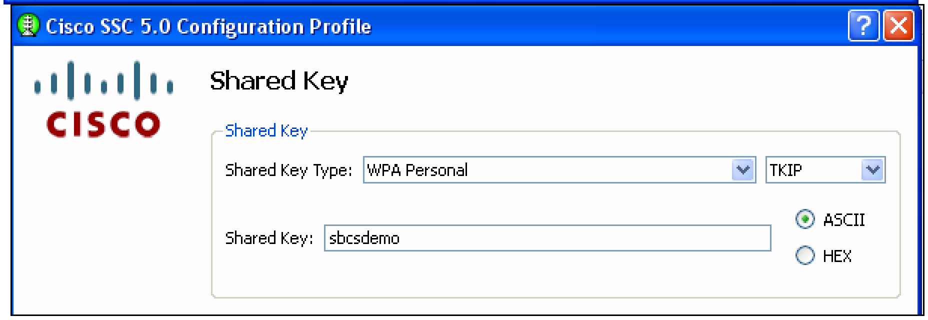
Open networks have no security, and are open to anybody within range. This is the least secure type of network.

● Shared Key Network

Shared Key Networks, use a shared key to encrypt data between end stations and network access points. This is a medium security level, suitable for small offices, or home offices.

○ Authenticating Network

Authentication networks provide the highest level of security and are perfect for enterprise level networks. Authentication networks require radius servers, and other network infrastructure.



Shared Key

Shared Key

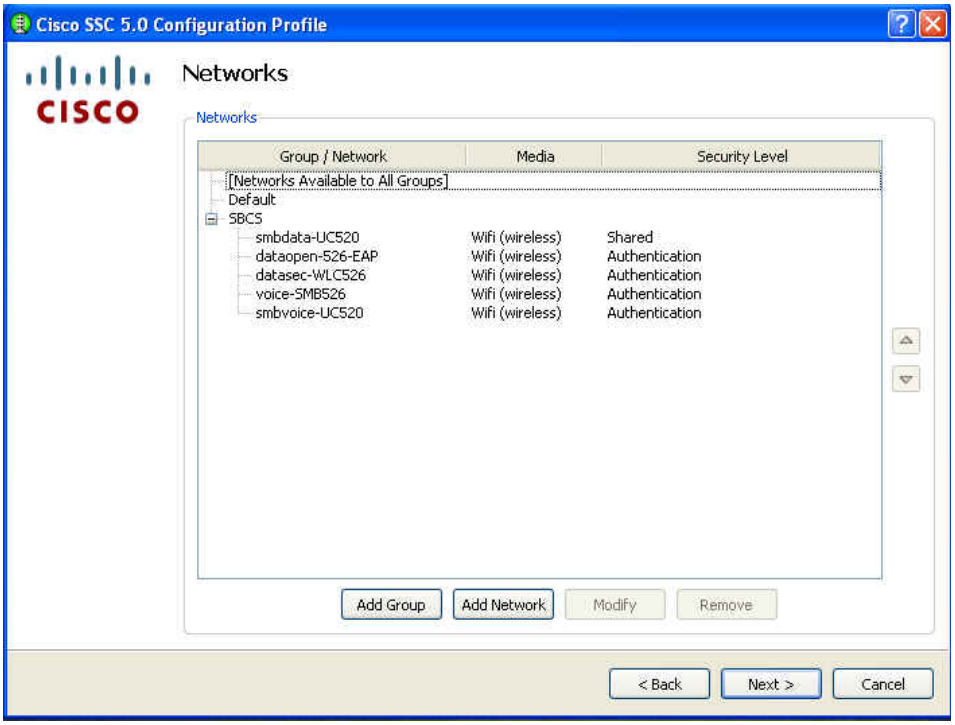
Shared Key Type: WPA Personal | TKIP

Shared Key: sbcsdemo

● ASCII

○ HEX

STEP 4. After finishing configuring the profile SBCS demo as shown above, save the profile to the SBCS group



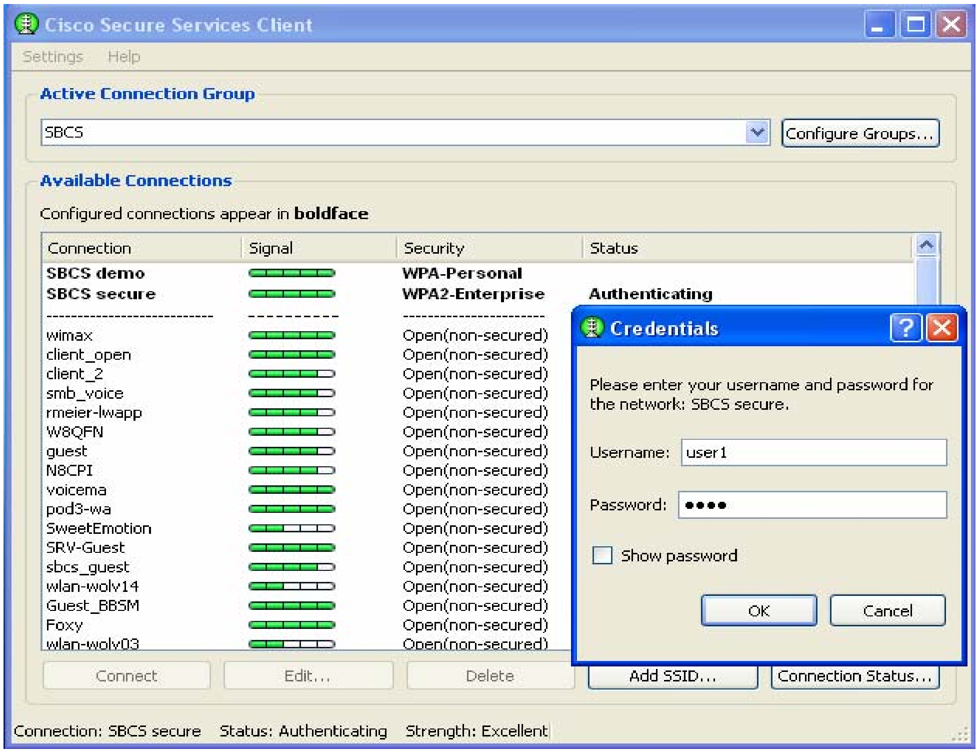
Cisco SSC 5.0 Configuration Profile

Networks

Networks

Group / Network	Media	Security Level
[Networks Available to All Groups]		
Default		
SBCS		
smbdata-UC520	Wifi (wireless)	Shared
dataopen-526-EAP	Wifi (wireless)	Authentication
datasec-WLC526	Wifi (wireless)	Authentication
voice-SMB526	Wifi (wireless)	Authentication
smbvoice-UC520	Wifi (wireless)	Authentication

STEP 5. In the next step after saving profile in the Configuration Manager, Start the CSSC Client Utility > Lunch the SBCS Demo profile and enter Authentication credentials when prompted.



Cisco Secure Services Client

Active Connection Group

SBCS

Available Connections

Configured connections appear in **boldface**

Connection	Signal	Security	Status
SBCS demo		**WPA-Personal**	
SBCS secure		**WPA2-Enterprise**	**Authenticating**
---------------------------	----------	----------------------	
wimax		Open(non-secured)	
client_open		Open(non-secured)	
client_2		Open(non-secured)	
smb_voice		Open(non-secured)	
rmeier-lwapp		Open(non-secured)	
W8QFN		Open(non-secured)	
guest		Open(non-secured)	
N8CPI		Open(non-secured)	
voicema		Open(non-secured)	
pod3-wa		Open(non-secured)	
SweetEmotion		Open(non-secured)	
SRV-Guest		Open(non-secured)	
sbcs_guest		Open(non-secured)	
wlan-wolv14		Open(non-secured)	
Guest_BBSM		Open(non-secured)	
Foxy		Open(non-secured)	
wlan-wolv03		Open(non-secured)	

Credentials

Please enter your username and password for the network: SBCS secure.

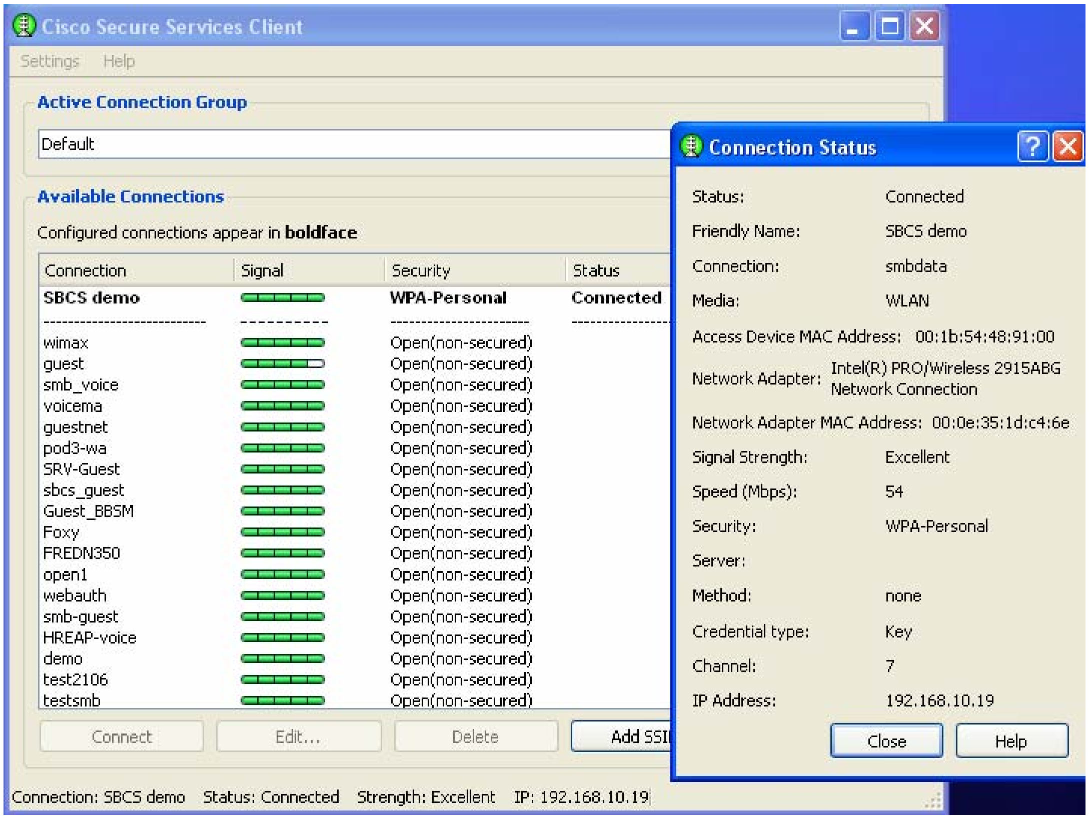
Username: user1

Password: ●●●●

☐ Show password

Connection: SBCS secure Status: Authenticating Strength: Excellent

STEP 6. And finally use the connection status tab to see the client IP address and other connectivity parameters as indicated in the screen shot below. The client received IP address fro the DHCP server on the UC 500 on VLAN 10.



Default

Configured connections appear in **boldface**

Connection	Signal	Security	Status
SBCS demo	▮▮▮▮▮	**WPA-Personal**	**Connected**
--------------------------	----------	----------------------	----------------
wimax	▮▮▮▮▮	Open(non-secured)	
guest	▮▮▮▮▯	Open(non-secured)	
smb_voice	▮▮▮▮▮	Open(non-secured)	
voicema	▮▮▮▮▮	Open(non-secured)	
guestnet	▮▮▮▮▮	Open(non-secured)	
pod3-wa	▮▮▮▮▮	Open(non-secured)	
SRV-Guest	▮▮▮▮▮	Open(non-secured)	
sbcs_guest	▮▮▮▮▮	Open(non-secured)	
Guest_BBSM	▮▮▮▮▮	Open(non-secured)	
Foxy	▮▮▮▮▮	Open(non-secured)	
FREDN350	▮▮▮▮▮	Open(non-secured)	
open1	▮▮▮▮▮	Open(non-secured)	
webauth	▮▮▮▮▮	Open(non-secured)	
smb-guest	▮▮▮▮▮	Open(non-secured)	
HREAP-voice	▮▮▮▮▮	Open(non-secured)	
demo	▮▮▮▮▮	Open(non-secured)	
test2106	▮▮▮▮▮	Open(non-secured)	
testsmb	▮▮▮▮▮	Open(non-secured)	

Connection: SBCS demo   Status: Connected   Strength: Excellent   IP: 192.168.10.19

Status:	Connected
Friendly Name:	SBCS demo
Connection:	smbdata
Media:	WLAN
Access Device MAC Address:	00:1b:54:48:91:00
Network Adapter:	Intel(R) PRO/Wireless 2915ABG Network Connection
Network Adapter MAC Address:	00:0e:35:1d:c4:6e
Signal Strength:	Excellent
Speed (Mbps):	54
Security:	WPA-Personal
Server:	
Method:	none
Credential type:	Key
Channel:	7
IP Address:	192.168.10.19

Wireless connectivity with UC 520 AP - Secure connectivity using MS Zero Config Supplicant

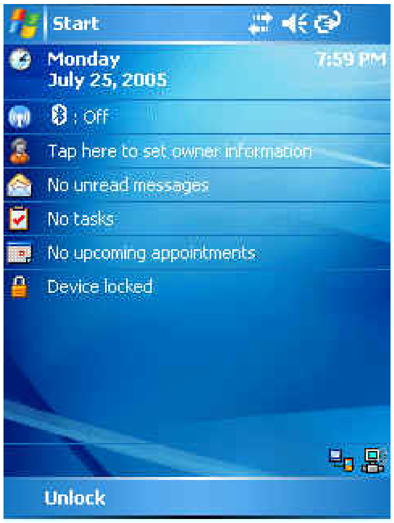
Next we can demonstrate setup with WPA/PSK on the hand held device. We will initially configure the Intermec CN-3 device with the Microsoft Wireless Zero Config supplicant that comes native on the Windows Mobile Device.

Note You can use any PDA or a Hand Held device that runs Windows CE Mobile if you don't have Intermec device for this demonstration

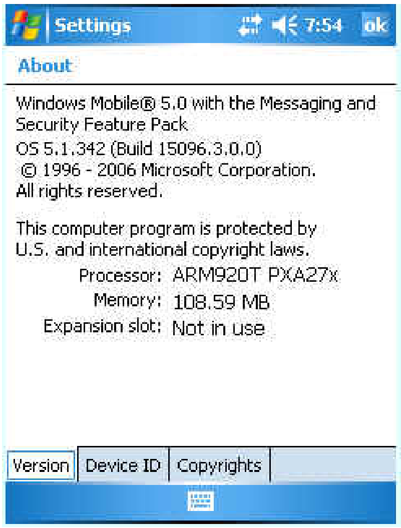
---

Note MS Zero config supports PEAP authentication however, Local Radius server on the UC520 supports only LEAP and EAP-FAST authentication methods therefore we cannot demonstrate PEAP with Windows Mobile.

STEP 1. We will demonstrate Wireless client connectivity with WPA/PSK on the Windows Mobile device.



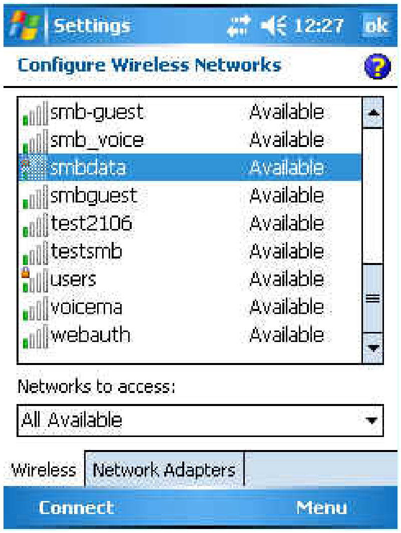
Monday
July 25, 2005 7:59 PM
: Off
Tap here to set owner information
No unread messages
No tasks
No upcoming appointments
Device locked



Windows Mobile® 5.0 with the Messaging and Security Feature Pack
OS 5.1.342 (Build 15096.3.0.0)
© 1996 - 2006 Microsoft Corporation.
All rights reserved.

This computer program is protected by U.S. and international copyright laws.

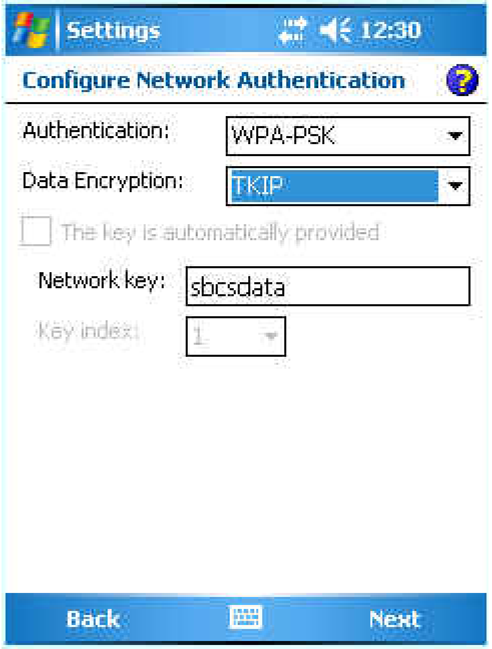
Processor:	ARM920T PXA27x
Memory:	108.59 MB
Expansion slot:	Not in use



smb-guest	Available
smb_voice	Available
smbdata	Available
smbguest	Available
test2106	Available
testsmb	Available
users	Available
voicema	Available
webauth	Available

Networks to access: All Available

STEP 2. Configure the discovered wireless network **smbdata with WPA/PSK.** Configure **SSID= smbdata** with **shared key=sbcsdata**



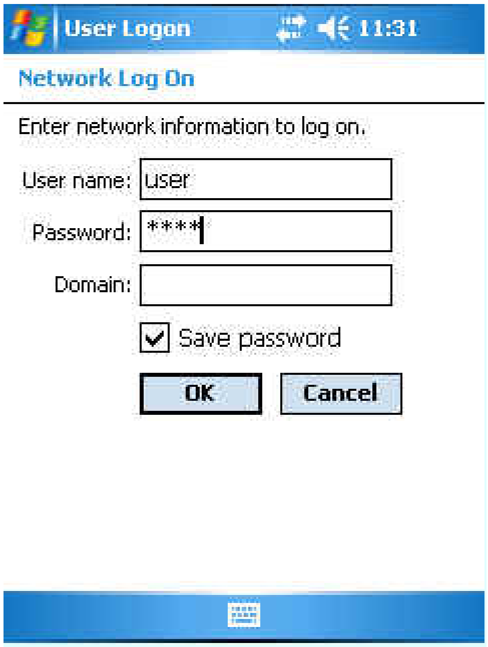
Authentication: WPA-PSK

Data Encryption: TKIP

□ The key is automatically provided

Network key: sbcsdata

Key index: 1



Enter network information to log on.

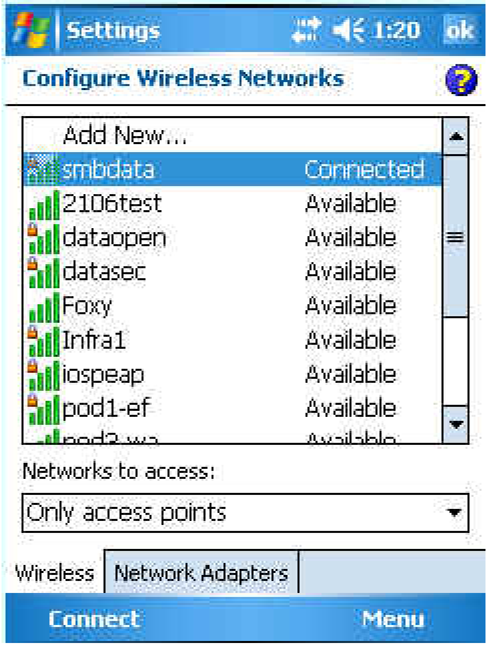
User name: user

Password: ****

Domain:

☑ Save password

STEP 3. After the user credential entered as shown above the client will authenticate and connect to the Wireless Network



Add New...

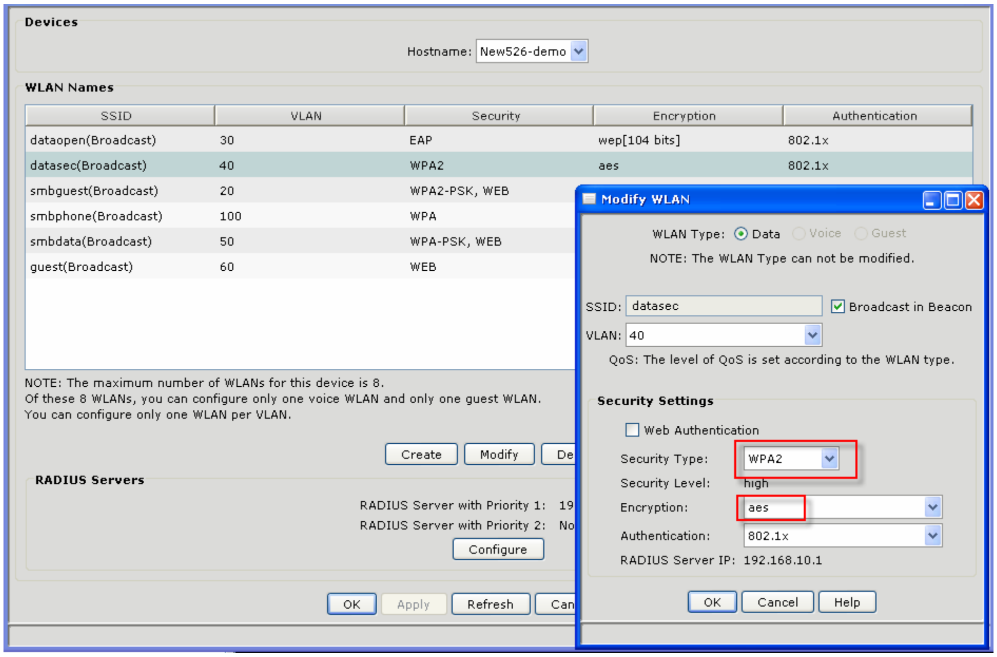
smbdata	Connected
2106test	Available
dataopen	Available
datasec	Available
Foxy	Available
Infra1	Available
iospeap	Available
pod1-ef	Available
pod2-wa	Available

Networks to access: Only access points

Wireless connectivity with WLC526 LAP - Secure connectivity using ADU and Odyssey Supplicants

Next we can demonstrate setup with WPA2/AES on the laptop and hand held device. For the next few client connectivity demonstration we will use WLC 526 controller and LWAPP APs.

STEP 1. We will demonstrate Wireless client connectivity with WPA2/AES and EAP-FAST authentication. Configure **SSID= datasec** with security WPA2/AES and EAP-FAST; in the security make sure Local RADIUS server 192.168.10.1 is configured with **key=demo**. See the configuration setup done with CCA 1.6 below.



Devices

Hostname: New526-demo

WLAN Names

SSID	VLAN	Security	Encryption	Authentication
dataopen(Broadcast)	30	EAP	wep[104 bits]	802.1x
datasec(Broadcast)	40	WPA2	aes	802.1x
smbguest(Broadcast)	20	WPA2-PSK, WEB		
smbphone(Broadcast)	100	WPA		
smbdata(Broadcast)	50	WPA-PSK, WEB		
guest(Broadcast)	60	WEB		

NOTE: The maximum number of WLANs for this device is 8.
Of these 8 WLANs, you can configure only one voice WLAN and only one guest WLAN.
You can configure only one WLAN per VLAN.

RADIUS Servers

RADIUS Server with Priority 1: 19
RADIUS Server with Priority 2: No

Modify WLAN

WLAN Type: ● Data ○ Voice ○ Guest

NOTE: The WLAN Type can not be modified.

SSID: datasec ☑ Broadcast in Beacon

VLAN: 40

QoS: The level of QoS is set according to the WLAN type.

Security Settings

□ Web Authentication

Security Type: WPA2

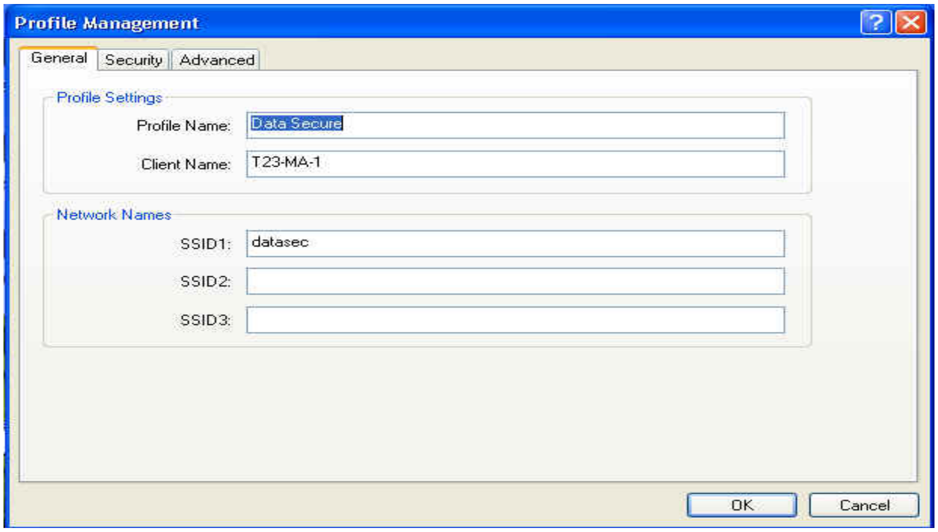
Security Level: high

Encryption: aes

Authentication: 802.1x

RADIUS Server IP: 192.168.10.1

STEP 2. Configure Client in ADU with the same credentials as shown above in step 1 in the CCA configuration. Create profile with a SSID=datasec.



Profile Management

Profile Settings

Profile Name: Data Secure

Client Name: T23-MA-1

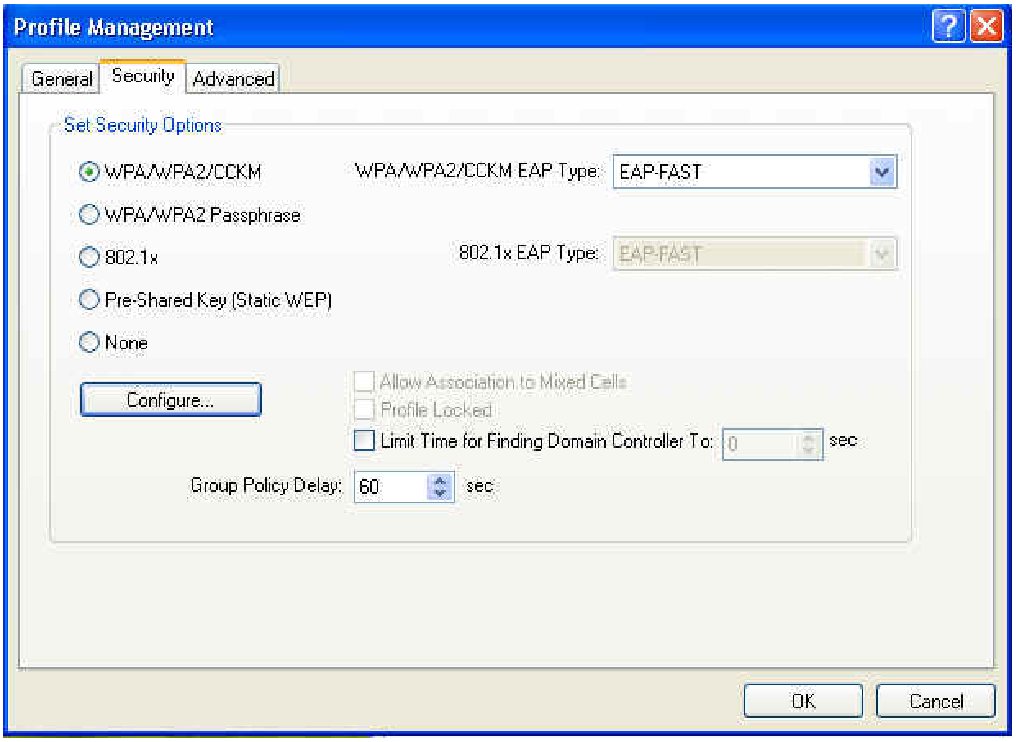
Network Names

SSID1: datasec

SSID2:

SSID3:

STEP 3. Configure in the ADU security settings for WPA2/AES and EAP-FAST authentication as shown below



Profile Management

General | Security | Advanced

Set Security Options

● WPA/WPA2/CCKM — WPA/WPA2/CCKM EAP Type: EAP-FAST

○ WPA/WPA2 Passphrase

○ 802.1x — 802.1x EAP Type: EAP-FAST

○ Pre-Shared Key (Static WEP)

○ None

Configure...

□ Allow Association to Mixed Cells

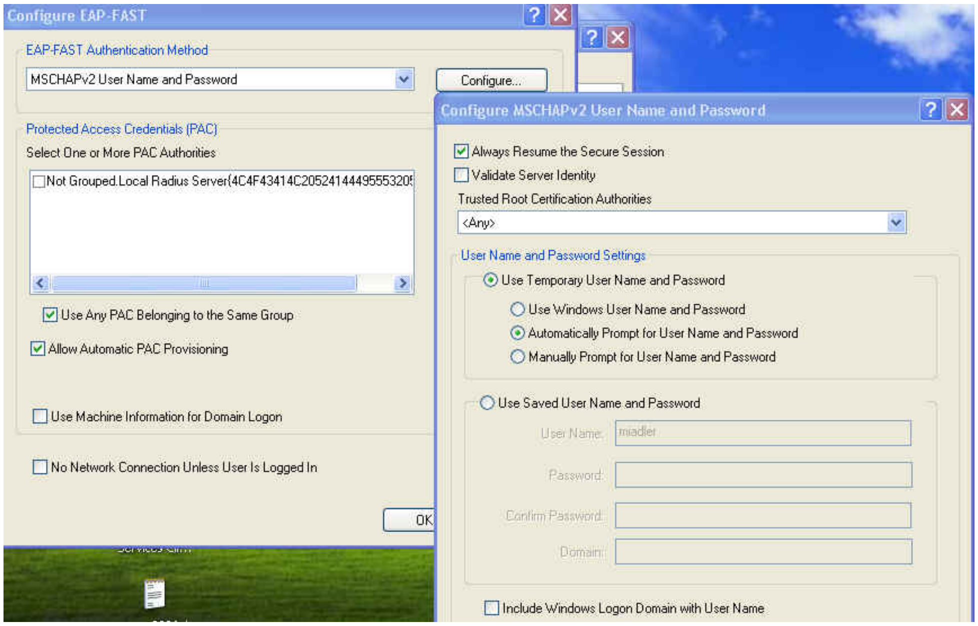
□ Profile Locked

□ Limit Time for Finding Domain Controller To: 0 sec

Group Policy Delay: 60 sec

OK | Cancel

STEP 4. Configure EAP-FAST settings as they are shown in the figure below



Configure EAP-FAST

EAP-FAST Authentication Method

MSCHAPv2 User Name and Password — Configure...

Protected Access Credentials (PAC)

Select One or More PAC Authorities

□ Not Grouped.Local Radius Server(4C4F43414C20524144495553205

☑ Use Any PAC Belonging to the Same Group

☑ Allow Automatic PAC Provisioning

□ Use Machine Information for Domain Logon

□ No Network Connection Unless User Is Logged In

OK

Configure MSCHAPv2 User Name and Password

☑ Always Resume the Secure Session

□ Validate Server Identity

Trusted Root Certification Authorities

<Any>

User Name and Password Settings

● Use Temporary User Name and Password

○ Use Windows User Name and Password

● Automatically Prompt for User Name and Password

○ Manually Prompt for User Name and Password

○ Use Saved User Name and Password

User Name: miadler

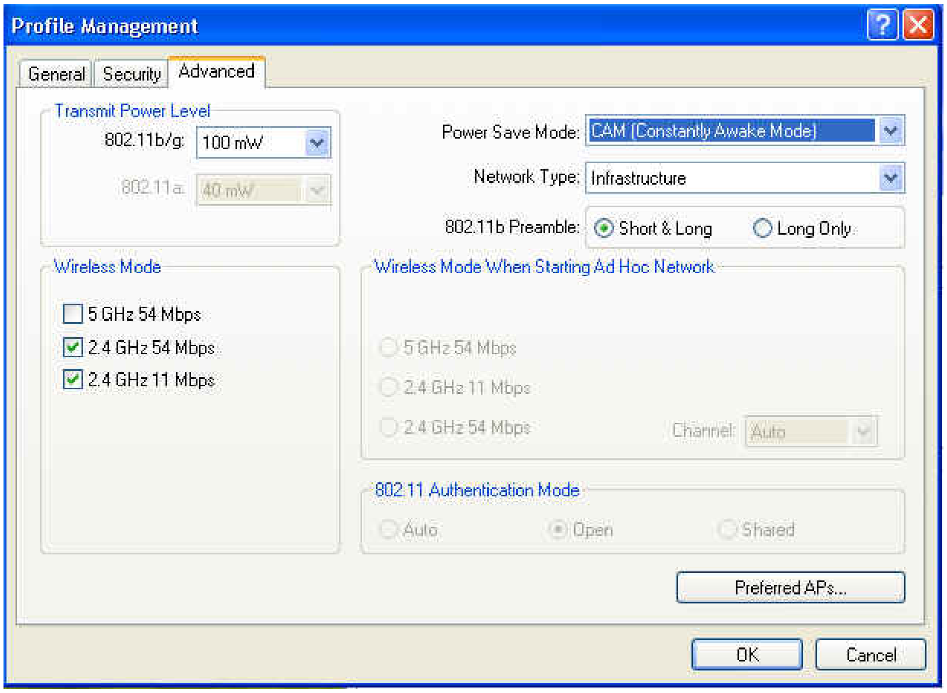
Password:

Confirm Password:

Domain:

□ Include Windows Logon Domain with User Name

STEP 5. In the Advanced option Tab you may want to configure additional options as shown and also disable the 5GHz scan since the 521 AP don’t support that mode.



Transmit Power Level
802.11b/g: 100 mW
802.11a: 40 mW

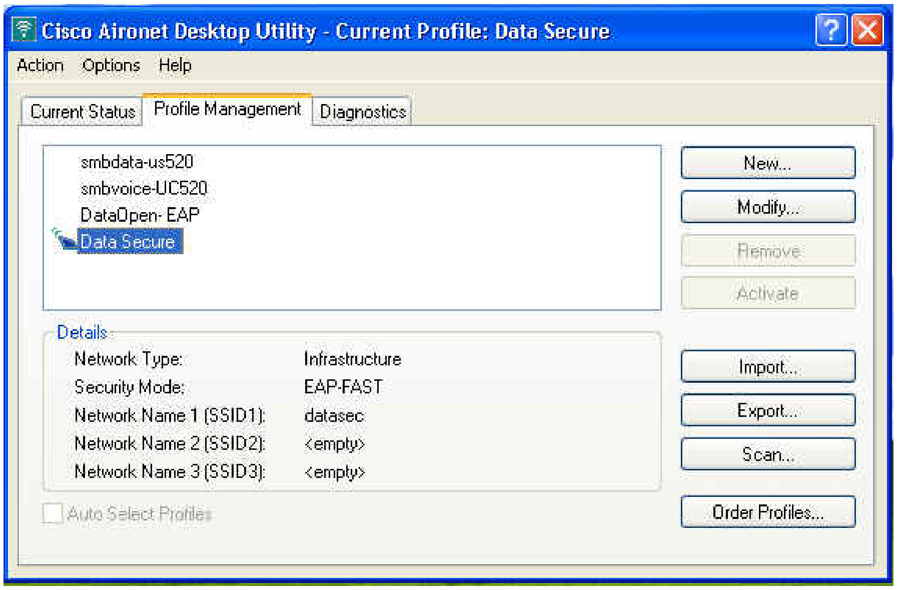
Power Save Mode: CAM (Constantly Awake Mode)
Network Type: Infrastructure
802.11b Preamble: ● Short & Long ○ Long Only

Wireless Mode
☐ 5 GHz 54 Mbps
☑ 2.4 GHz 54 Mbps
☑ 2.4 GHz 11 Mbps

Wireless Mode When Starting Ad Hoc Network
○ 5 GHz 54 Mbps
○ 2.4 GHz 11 Mbps
○ 2.4 GHz 54 Mbps
Channel: Auto

802.11 Authentication Mode
○ Auto ● Open ○ Shared

STEP 6. Finally activate the newly created profile

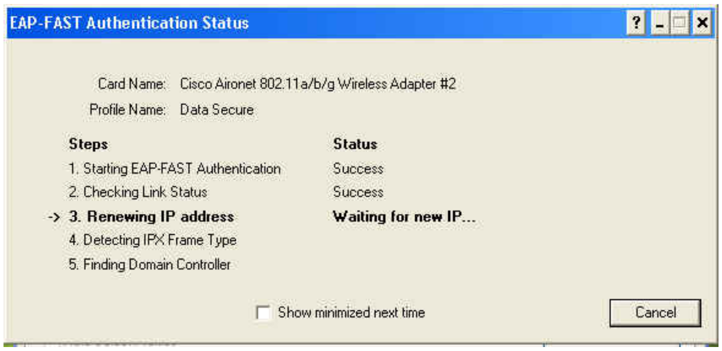


smbdata-us520
smbvoice-UC520
DataOpen- EAP
Data Secure

Details
Network Type: Infrastructure
Security Mode: EAP-FAST
Network Name 1 (SSID1): datasec
Network Name 2 (SSID2): <empty>
Network Name 3 (SSID3): <empty>

☐ Auto Select Profiles

STEP 7. The wireless client should Associate, Authenticate and eventually get an IP address from the DHCP server on VLAN 40.



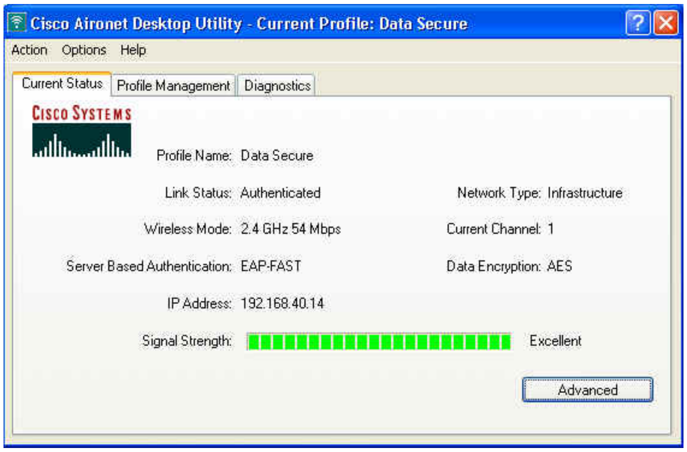
EAP-FAST Authentication Status

Card Name: Cisco Aironet 802.11a/b/g Wireless Adapter #2

Profile Name: Data Secure

Steps	Status
1. Starting EAP-FAST Authentication	Success
2. Checking Link Status	Success
-> **3. Renewing IP address**	**Waiting for new IP...**
4. Detecting IPX Frame Type	
5. Finding Domain Controller	

☐ Show minimized next time



Cisco Aironet Desktop Utility - Current Profile: Data Secure

Profile Name: Data Secure

Link Status: Authenticated

Network Type: Infrastructure

Wireless Mode: 2.4 GHz 54 Mbps

Current Channel: 1

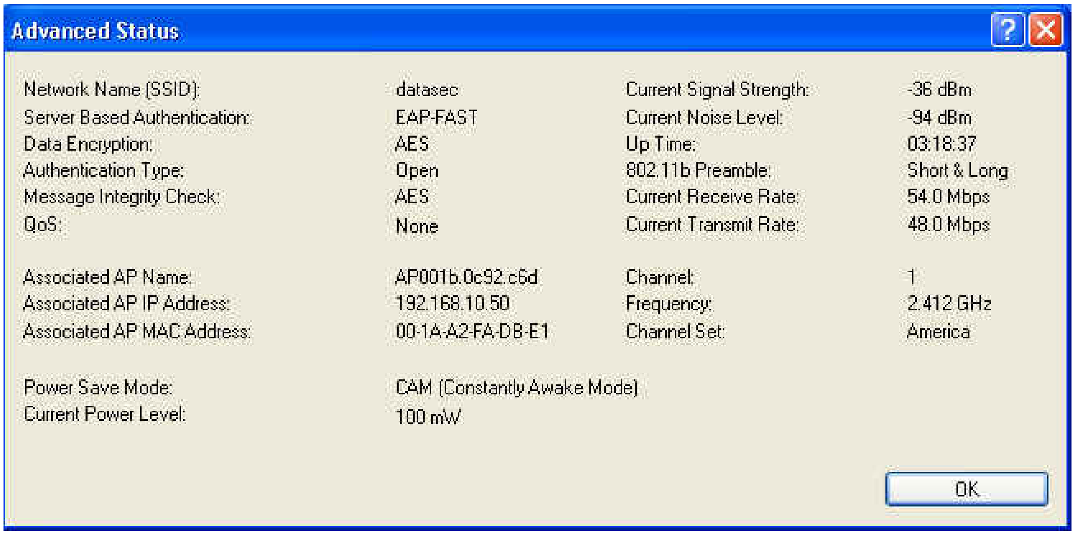
Server Based Authentication: EAP-FAST

Data Encryption: AES

IP Address: 192.168.40.14

Signal Strength: Excellent

STEP 8. In Web UI interface you can show more details about the connected client and even do a Link Test. And also on the Client device in ADU you can see in more Advanced Status tab.

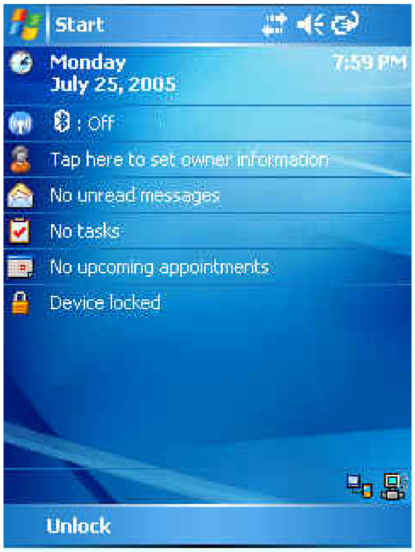


Advanced Status

Network Name (SSID):	datasec	Current Signal Strength:	-36 dBm
Server Based Authentication:	EAP-FAST	Current Noise Level:	-94 dBm
Data Encryption:	AES	Up Time:	03:18:37
Authentication Type:	Open	802.11b Preamble:	Short & Long
Message Integrity Check:	AES	Current Receive Rate:	54.0 Mbps
QoS:	None	Current Transmit Rate:	48.0 Mbps
Associated AP Name:	AP001b.0c92.c6d	Channel:	1
Associated AP IP Address:	192.168.10.50	Frequency:	2.412 GHz
Associated AP MAC Address:	00-1A-A2-FA-DB-E1	Channel Set:	America
Power Save Mode:	CAM (Constantly Awake Mode)		
Current Power Level:	100 mW		

Client Connectivity using Intermec CN-3 device and Odyssey or Windows Mobile supplicant

STEP 1. Configure the CN-3 device using the Odyssey interface for the WPA2/AES and EAP_FAST authentication



Start

Monday
July 25, 2005 7:59 PM

: Off

Tap here to set owner information

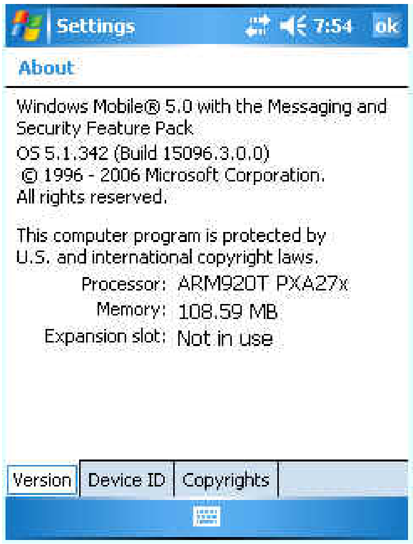
No unread messages

No tasks

No upcoming appointments

Device locked

Unlock



Settings 7:54 ok

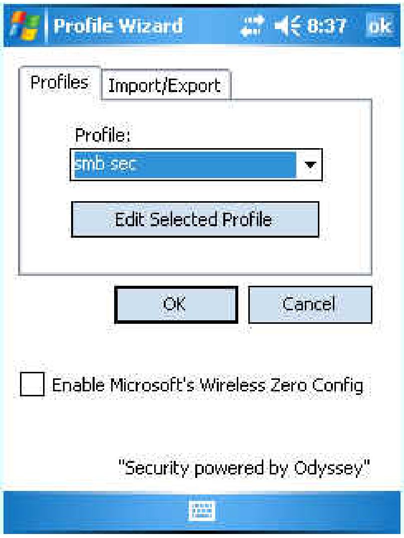
About

Windows Mobile® 5.0 with the Messaging and Security Feature Pack
OS 5.1.342 (Build 15096.3.0.0)
© 1996 - 2006 Microsoft Corporation.
All rights reserved.

This computer program is protected by U.S. and international copyright laws.

Processor:	ARM920T PXA27x
Memory:	108.59 MB
Expansion slot:	Not in use

Version | Device ID | Copyrights



Profile Wizard 8:37 ok

Profiles | Import/Export

Profile: smb sec

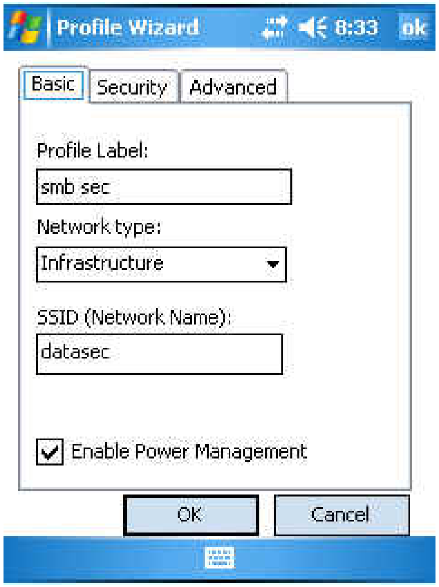
Edit Selected Profile

OK | Cancel

□ Enable Microsoft's Wireless Zero Config

"Security powered by Odyssey"

STEP 2. Configure the Odyssey with **SSID= datasec** withWPA2/AES and EAP-FAST



Profile Wizard 8:33 ok

Basic | Security | Advanced

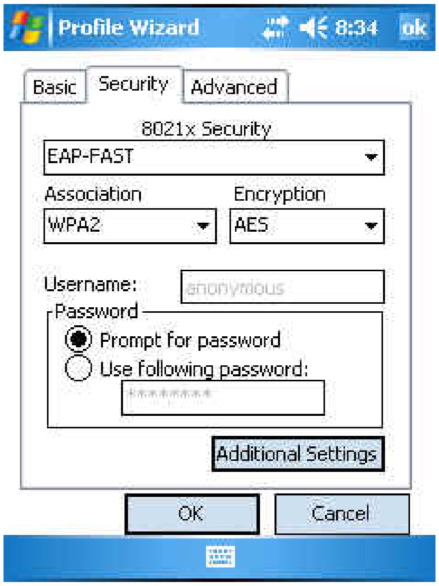
Profile Label: smb sec

Network type: Infrastructure

SSID (Network Name): datasec

☑ Enable Power Management

OK | Cancel



Profile Wizard 8:34 ok

Basic | Security | Advanced

8021x Security: EAP-FAST

Association: WPA2

Encryption: AES

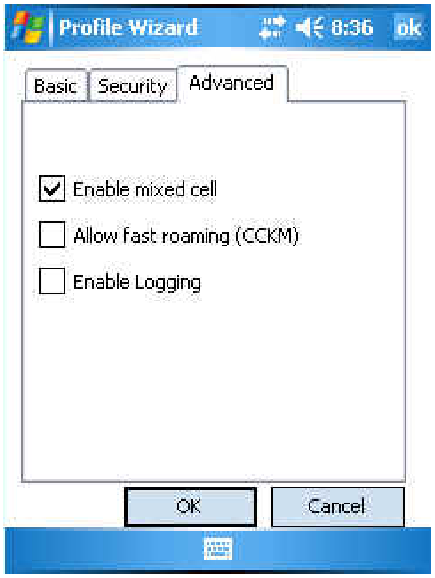
Username: anonymous

Password

● Prompt for password
○ Use following password: ********

Additional Settings

OK | Cancel



Profile Wizard 8:36 ok

Basic | Security | Advanced

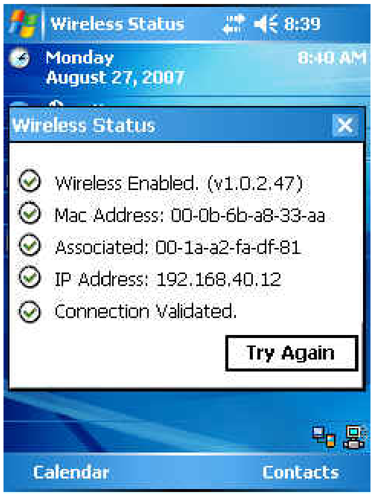
☑ Enable mixed cell

□ Allow fast roaming (CCKM)

□ Enable Logging

OK | Cancel

STEP 3. After you entered authentication credentials **user=user5 and passw=demo** as it was configured on the Local Radius Server you will see the client Associate, Authenticate and receiving IP address.

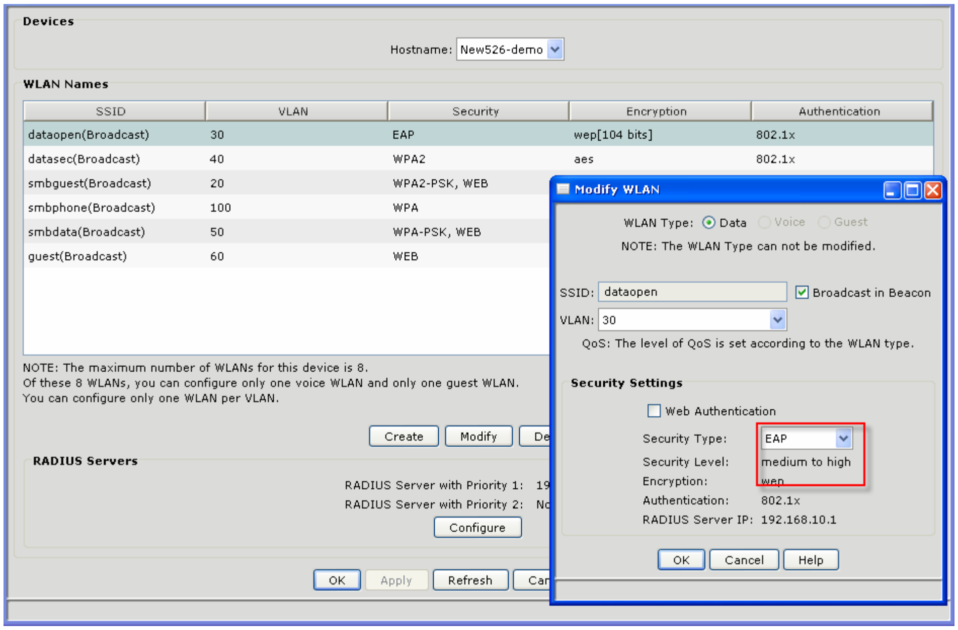


Wireless Status

✓ Wireless Enabled. (v1.0.2.47)
✓ Mac Address: 00-0b-6b-a8-33-aa
✓ Associated: 00-1a-a2-fa-df-81
✓ IP Address: 192.168.40.12
✓ Connection Validated.

Wireless Client Connectivity with WLC 526 and LAP using Cisco 350 card and ACU with EAP/WEP

STEP 1. In this demonstration we will show client connectivity to the Wireless Network with SSID=dataopen with EAP/Dynamic WEP configured with CCA.



Devices

Hostname: New526-demo

WLAN Names

SSID	VLAN	Security	Encryption	Authentication
dataopen(Broadcast)	30	EAP	wep[104 bits]	802.1x
datasec(Broadcast)	40	WPA2	aes	802.1x
smbguest(Broadcast)	20	WPA2-PSK, WEB		
smbphone(Broadcast)	100	WPA		
smbdata(Broadcast)	50	WPA-PSK, WEB		
guest(Broadcast)	60	WEB		

NOTE: The maximum number of WLANs for this device is 8.
Of these 8 WLANs, you can configure only one voice WLAN and only one guest WLAN.
You can configure only one WLAN per VLAN.

RADIUS Servers

RADIUS Server with Priority 1: 19
RADIUS Server with Priority 2: No

Modify WLAN

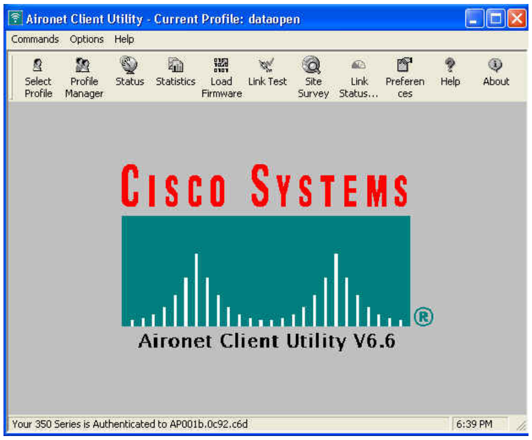
WLAN Type: ● Data ○ Voice ○ Guest
NOTE: The WLAN Type can not be modified.

SSID: dataopen ☑ Broadcast in Beacon
VLAN: 30
QoS: The level of QoS is set according to the WLAN type.

Security Settings

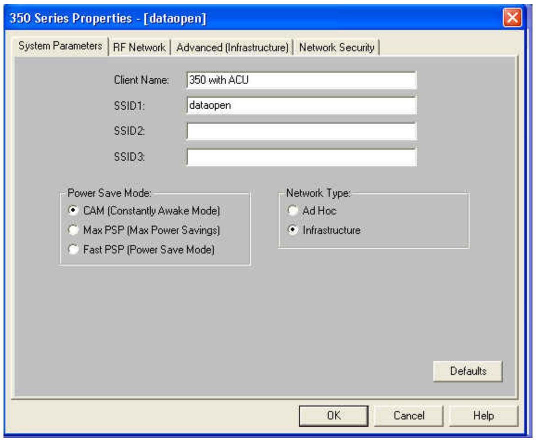
☐ Web Authentication
Security Type: EAP
Security Level: medium to high
Encryption: wep
Authentication: 802.1x
RADIUS Server IP: 192.168.10.1

STEP 2. Configure Cisco Wireless Client with the same SSID=dataopen using ACU 6.6 . Create a profile **350 with ACU** in the ACU under Profile Manager Menu option as shown below.



Aironet Client Utility - Current Profile: dataopen

Your 350 Series is Authenticated to AP001b.0c92.c6d | 6:39 PM



350 Series Properties - [dataopen]

Client Name: 350 with ACU

SSID1: dataopen

SSID2:

SSID3:

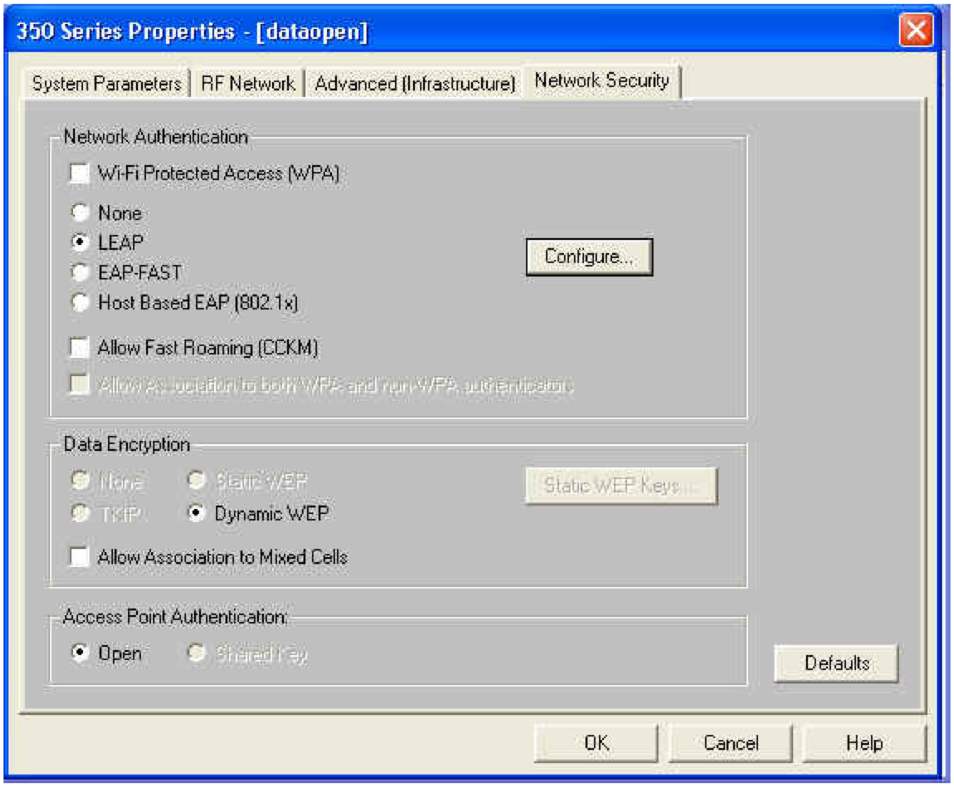
Power Save Mode:

- ● CAM (Constantly Awake Mode)
- ○ Max PSP (Max Power Savings)
- ○ Fast PSP (Power Save Mode)

Network Type:

- ○ Ad Hoc
- ● Infrastructure

STEP 3. Configure wireless security as LEAP under Network Security Tab in the ACU and then configure LEAP.



350 Series Properties - [dataopen]

Network Authentication

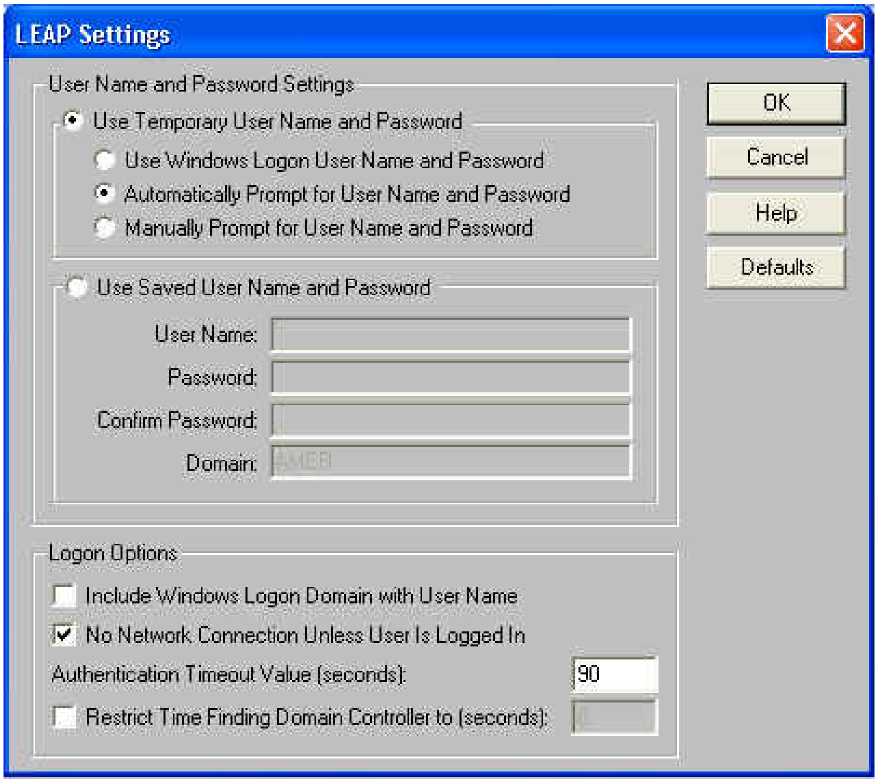
- □ Wi-Fi Protected Access (WPA)
- ○ None
- ● LEAP
- ○ EAP-FAST
- ○ Host Based EAP (802.1x)
- □ Allow Fast Roaming (CCKM)
- □ Allow Association to both WPA and non-WPA authentication

Data Encryption

- ○ None ○ Static WEP
- ○ TKIP ● Dynamic WEP
- □ Allow Association to Mixed Cells

Access Point Authentication

- ● Open ○ Shared Key



LEAP Settings

User Name and Password Settings

● Use Temporary User Name and Password

○ Use Windows Logon User Name and Password

● Automatically Prompt for User Name and Password

○ Manually Prompt for User Name and Password

○ Use Saved User Name and Password

User Name:

Password:

Confirm Password:

Domain: AMER

Logon Options

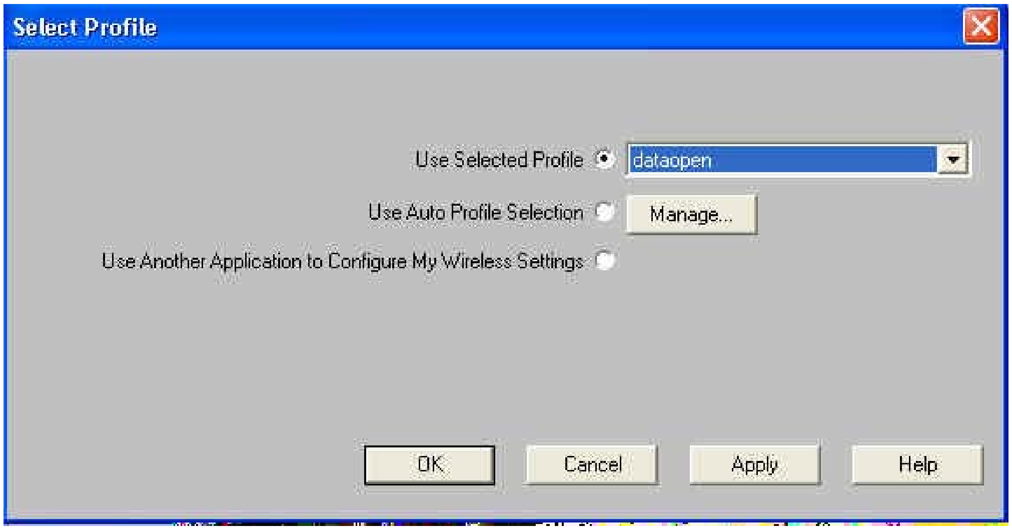
□ Include Windows Logon Domain with User Name

☑ No Network Connection Unless User Is Logged In

Authentication Timeout Value (seconds): 90

□ Restrict Time Finding Domain Controller to (seconds):

STEP 4. Save the profile and then select it in the ACU main menu using Select Profile option.



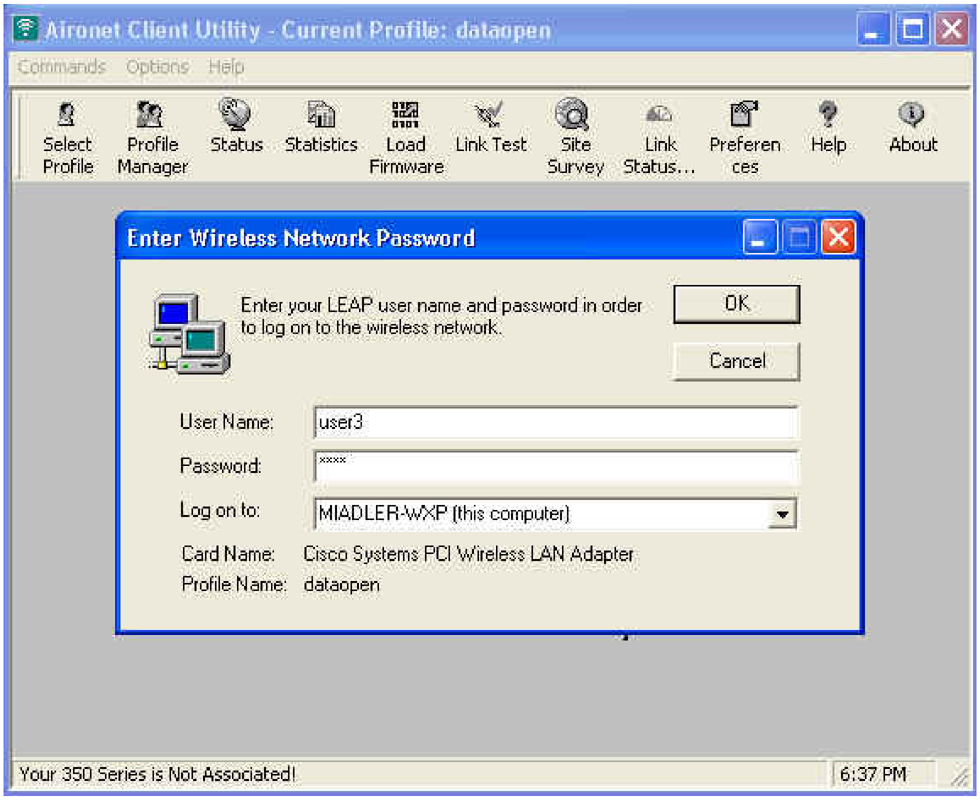
Select Profile

Use Selected Profile ● dataopen

Use Auto Profile Selection ○

Use Another Application to Configure My Wireless Settings ○

STEP 5. Authenticate to the wireless network with credentials as configured on the Local Radius server on the UC520. User **name=user3 and password=demo**



Enter your LEAP user name and password in order to log on to the wireless network.

User Name: user3

Password: ****

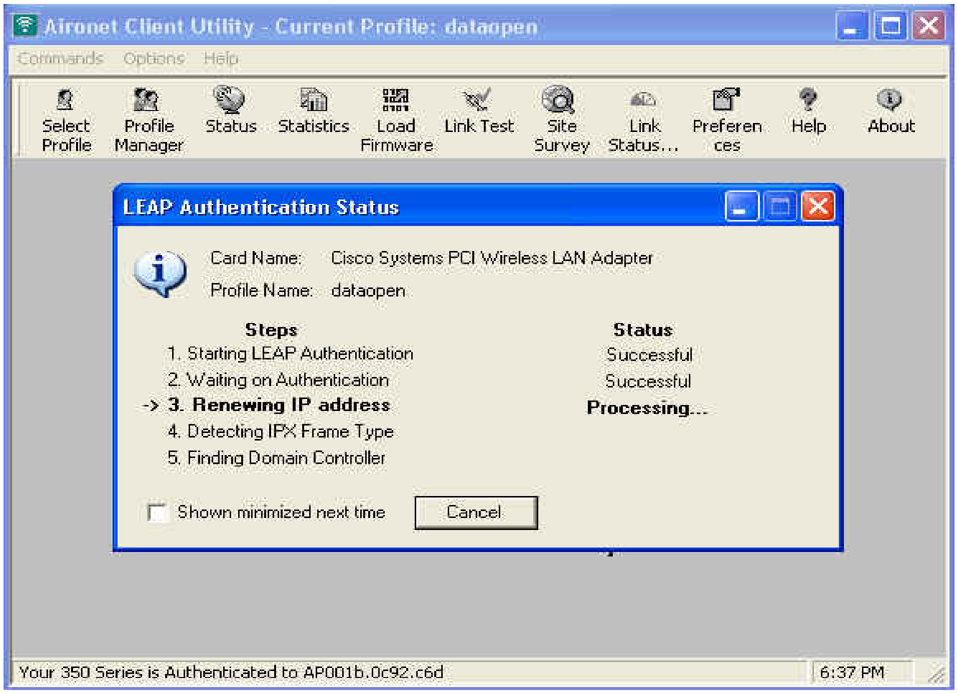
Log on to: MIADLER-WXP (this computer)

Card Name: Cisco Systems PCI Wireless LAN Adapter

Profile Name: dataopen

Your 350 Series is Not Associated! 6:37 PM

STEP 6. The client will Authenticate and receive IP address from the DHCP server configured on the UC520 on the VLAN 30



Card Name: Cisco Systems PCI Wireless LAN Adapter

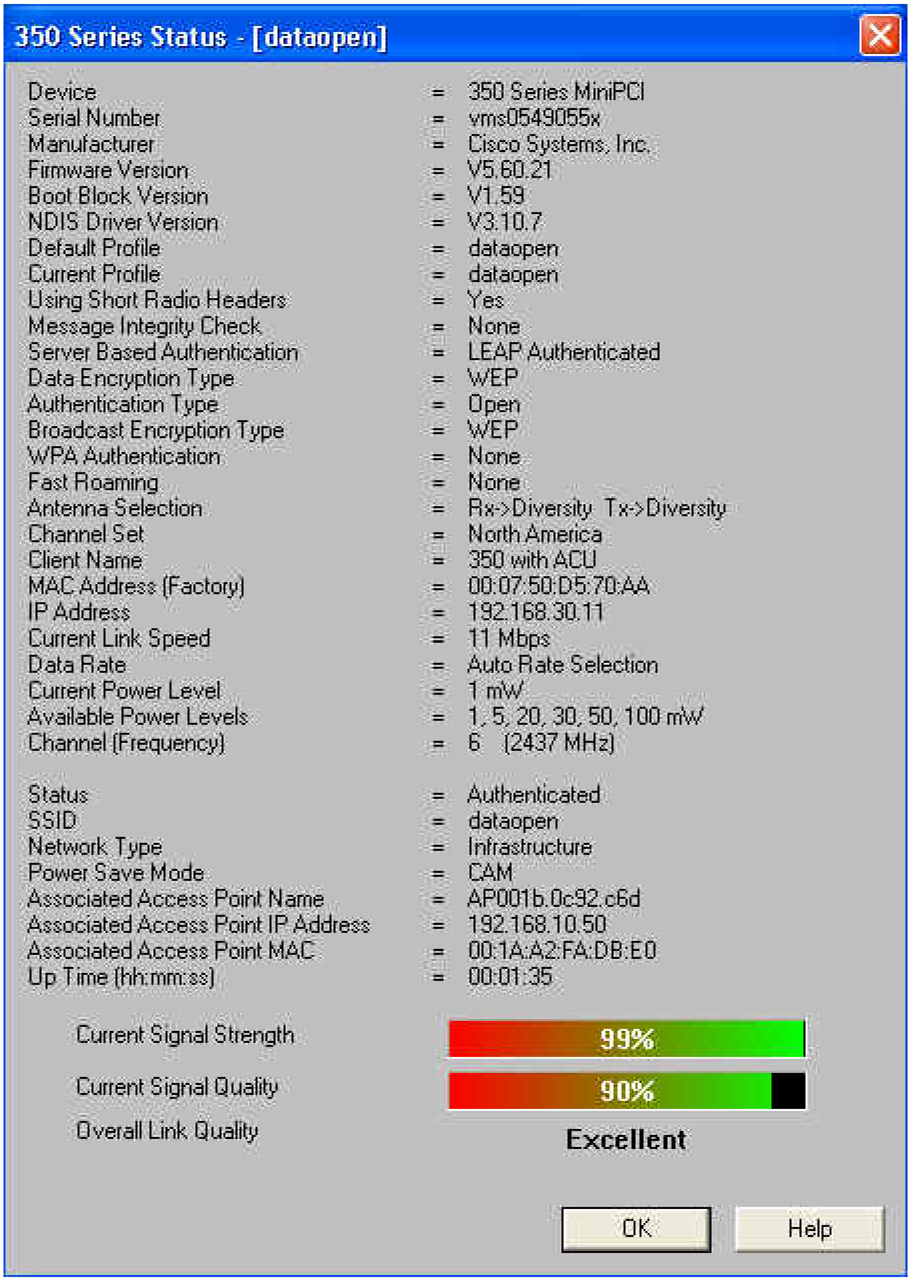
Profile Name: dataopen

Steps	Status
1. Starting LEAP Authentication	Successful
2. Waiting on Authentication	Successful
-> **3. Renewing IP address**	**Processing...**
4. Detecting IPX Frame Type	
5. Finding Domain Controller	

□ Shown minimized next time

Your 350 Series is Authenticated to AP001b.0c92.c6d 6:37 PM

STEP 7. And finally verify the connectivity in the ACU main menu under the Status tab.



350 Series Status - [dataopen]

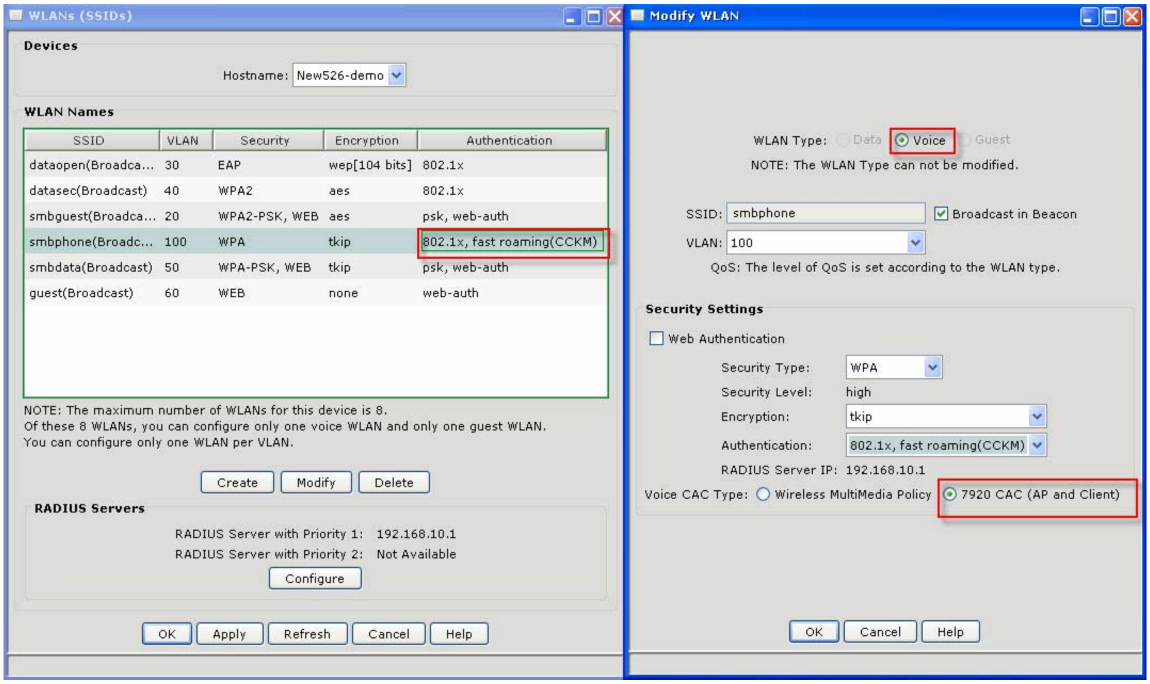
```
Device                                  =   350 Series MiniPCI
Serial Number                           =   vms0549055x
Manufacturer                            =   Cisco Systems, Inc.
Firmware Version                        =   V5.60.21
Boot Block Version                      =   V1.59
NDIS Driver Version                     =   V3.10.7
Default Profile                         =   dataopen
Current Profile                         =   dataopen
Using Short Radio Headers               =   Yes
Message Integrity Check                 =   None
Server Based Authentication             =   LEAP Authenticated
Data Encryption Type                    =   WEP
Authentication Type                     =   Open
Broadcast Encryption Type               =   WEP
WPA Authentication                      =   None
Fast Roaming                            =   None
Antenna Selection                       =   Rx->Diversity  Tx->Diversity
Channel Set                             =   North America
Client Name                             =   350 with ACU
MAC Address (Factory)                   =   00:07:50:D5:70:AA
IP Address                              =   192.168.30.11
Current Link Speed                      =   11 Mbps
Data Rate                               =   Auto Rate Selection
Current Power Level                     =   1 mW
Available Power Levels                  =   1, 5, 20, 30, 50, 100 mW
Channel (Frequency)                     =   6   (2437 MHz)

Status                                  =   Authenticated
SSID                                    =   dataopen
Network Type                            =   Infrastructure
Power Save Mode                         =   CAM
Associated Access Point Name            =   AP001b.0c92.c6d
Associated Access Point IP Address      =   192.168.10.50
Associated Access Point MAC             =   00:1A:A2:FA:DB:E0
Up Time (hh:mm:ss)                      =   00:01:35

    Current Signal Strength                 99%

    Current Signal Quality                  90%

    Overall Link Quality                    Excellent
```

Wireless connectivity with WLC526 LAP521 - Secure connectivity using Wireless 7921 Phones

Next we can demonstrate setup with WPA/TKIP and 802.1x with Wireless Phone clients. We will initially configure the Cisco 7921 device with the GUI interface on the phone supplicant that comes native on the 7921.

Note It is technically difficult to get the screen shots from the 7921; therefore we will demonstrate the configuration setup of the 7921 using Browser interface connecting to the 7921.

Note In the CCA version 1.6 there is now a new capability to configure some Advances VoIP features for the Wireless Clients. The Advanced Voice features such as CAC (Call Admission Control) and the Fast Secure Roaming (CCKM) can be configured right in the CCA 1.6 interface as shown below.



WLANs (SSIDs)

Devices

Hostname: New526-demo

WLAN Names

SSID	VLAN	Security	Encryption	Authentication
dataopen(Broadca...	30	EAP	wep[104 bits]	802.1x
datasec(Broadcast)	40	WPA2	aes	802.1x
smbguest(Broadca...	20	WPA2-PSK, WEB	aes	psk, web-auth
smbphone(Broadc...	100	WPA	tkip	802.1x, fast roaming(CCKM)
smbdata(Broadcast)	50	WPA-PSK, WEB	tkip	psk, web-auth
guest(Broadcast)	60	WEB	none	web-auth

NOTE: The maximum number of WLANs for this device is 8.
Of these 8 WLANs, you can configure only one voice WLAN and only one guest WLAN.
You can configure only one WLAN per VLAN.

RADIUS Servers

RADIUS Server with Priority 1: 192.168.10.1
RADIUS Server with Priority 2: Not Available

Modify WLAN

WLAN Type: ○ Data ● Voice ○ Guest
NOTE: The WLAN Type can not be modified.

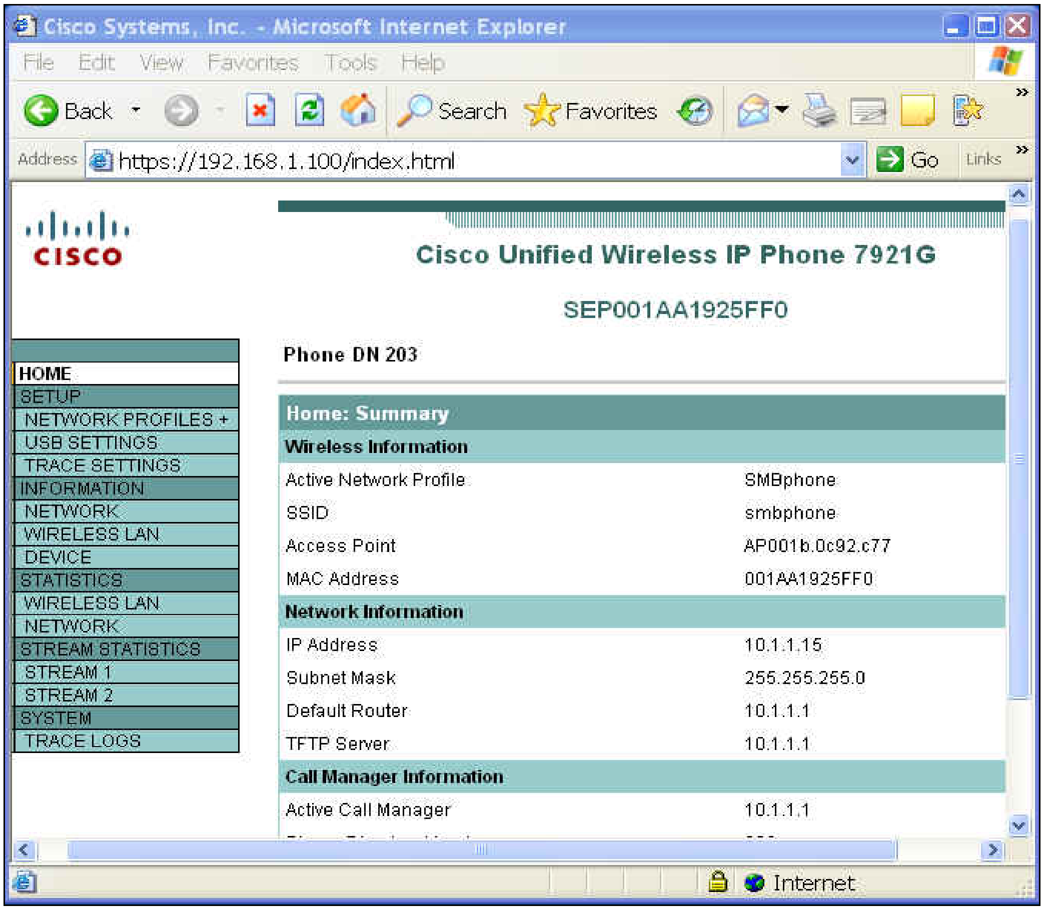
SSID: smbphone ☑ Broadcast in Beacon
VLAN: 100
QoS: The level of QoS is set according to the WLAN type.

Security Settings

☐ Web Authentication

Security Type: WPA
Security Level: high
Encryption: tkip
Authentication: 802.1x, fast roaming(CCKM)
RADIUS Server IP: 192.168.10.1
Voice CAC Type: ○ Wireless MultiMedia Policy ● 7920 CAC (AP and Client)

STEP 1. We will demonstrate 7921 client connectivity to the SSID=**smbphone** in the CCA 1.6. Other settings on the 7921 are for the Default Router 10.1.1.1 and CME(Call Manager Express) – 10.1.1.1. As shown below the client IP address 10.1.1.15, note the IP address may be different!


Cisco Systems, Inc. - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
https://192.168.1.100/index.html
Go
Links
CISCO
Internet

Cisco Unified Wireless IP Phone 7921G

SEP001AA1925FF0

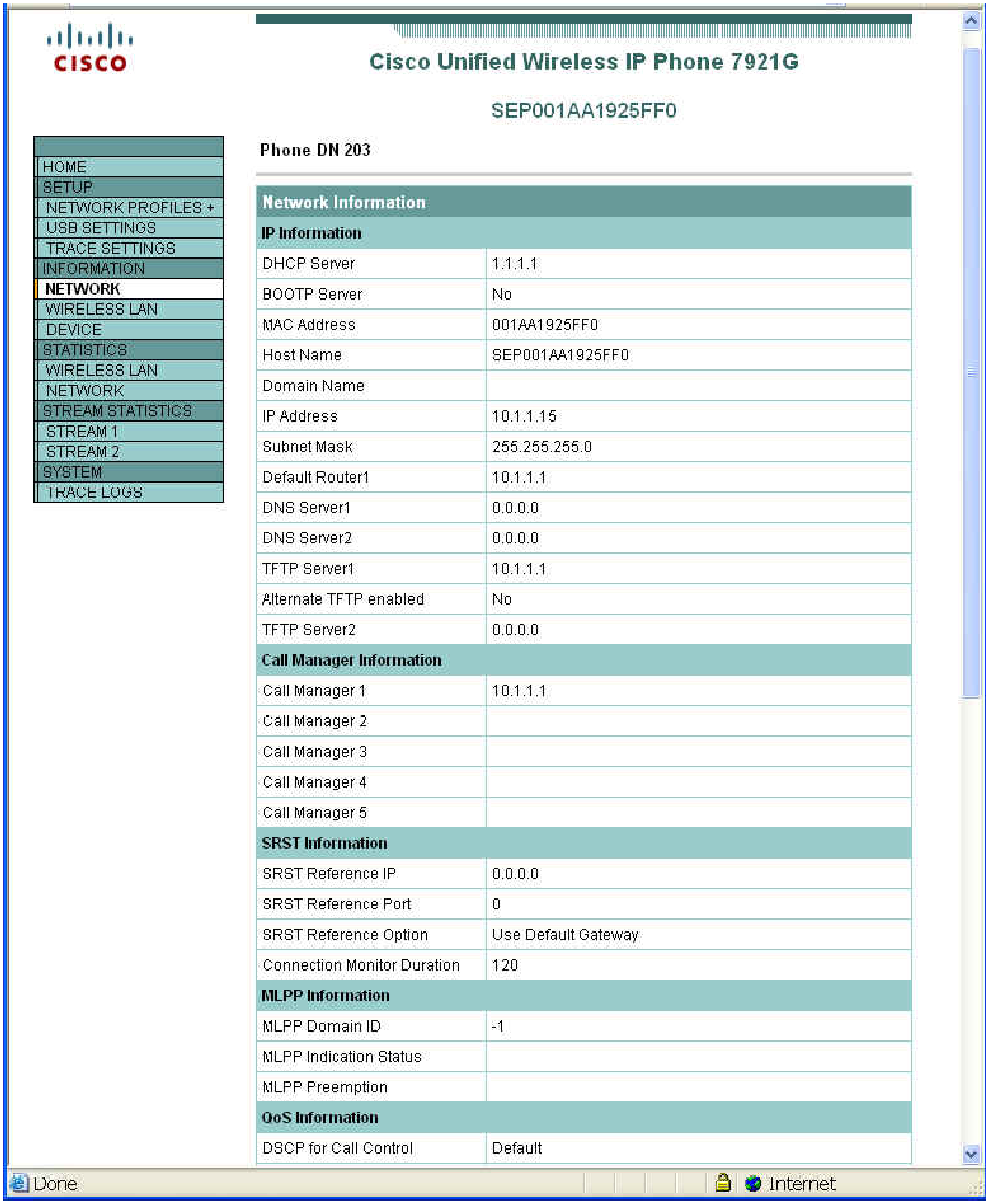
Phone DN 203

- HOME
- SETUP
  - NETWORK PROFILES +
  - USB SETTINGS
  - TRACE SETTINGS
- INFORMATION
  - NETWORK
  - WIRELESS LAN
  - DEVICE
- STATISTICS
  - WIRELESS LAN
  - NETWORK
- STREAM STATISTICS
  - STREAM 1
  - STREAM 2
- SYSTEM
  - TRACE LOGS

Home: Summary

Wireless Information	
Active Network Profile	SMBphone
SSID	smbphone
Access Point	AP001b.0c92.c77
MAC Address	001AA1925FF0
Network Information	
IP Address	10.1.1.15
Subnet Mask	255.255.255.0
Default Router	10.1.1.1
TFTP Server	10.1.1.1
Call Manager Information	
Active Call Manager	10.1.1.1

STEP 2. Configure the Active Profile SMBphone with SSID= **smbphone**



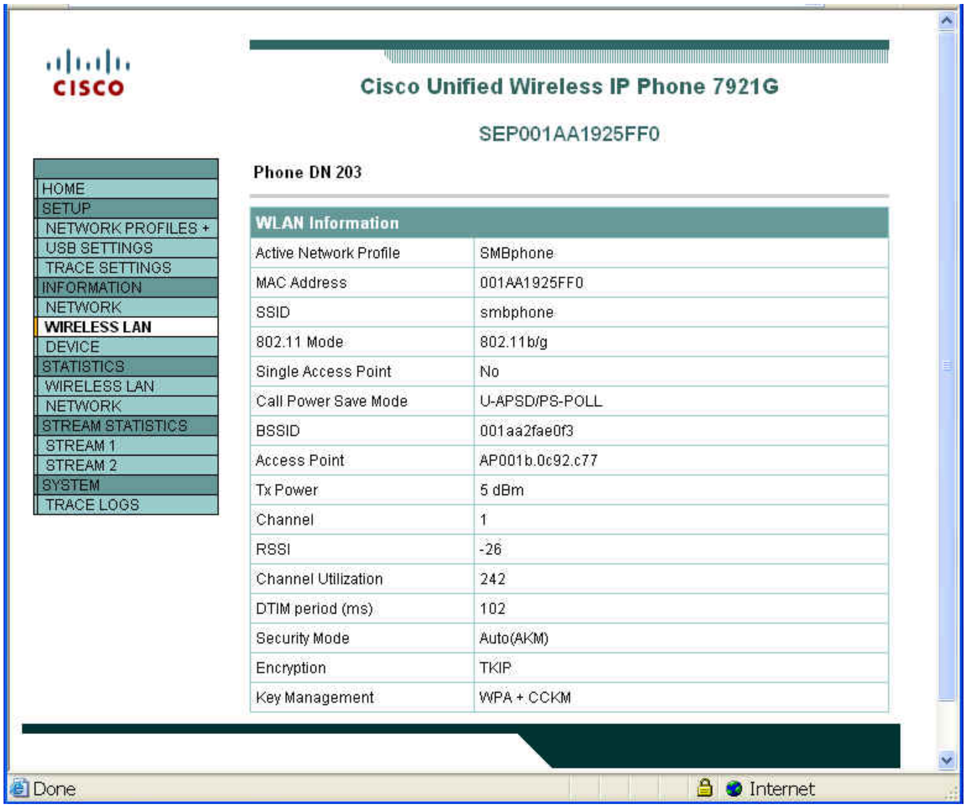
Cisco Unified Wireless IP Phone 7921G

SEP001AA1925FF0

Phone DN 203

Network Information	
IP Information	
DHCP Server	1.1.1.1
BOOTP Server	No
MAC Address	001AA1925FF0
Host Name	SEP001AA1925FF0
Domain Name	
IP Address	10.1.1.15
Subnet Mask	255.255.255.0
Default Router1	10.1.1.1
DNS Server1	0.0.0.0
DNS Server2	0.0.0.0
TFTP Server1	10.1.1.1
Alternate TFTP enabled	No
TFTP Server2	0.0.0.0
Call Manager Information	
Call Manager 1	10.1.1.1
Call Manager 2	
Call Manager 3	
Call Manager 4	
Call Manager 5	
SRST Information	
SRST Reference IP	0.0.0.0
SRST Reference Port	0
SRST Reference Option	Use Default Gateway
Connection Monitor Duration	120
MLPP Information	
MLPP Domain ID	-1
MLPP Indication Status	
MLPP Preemption	
QoS Information	
DSCP for Call Control	Default

STEP 3. On the 7921 create a Wireless Profile SMBphone and setup the wireless options as shown below. Security should be setup to WPA/TKIP and Authentication Auto AKM equivalent to CCKM (Cisco Centralized Key Management = Fast Secure Roaming). When Auto AKM is selected on the 7921 phone the Authentication type will be LEAP automatically as it will show below in the controller screen shot.



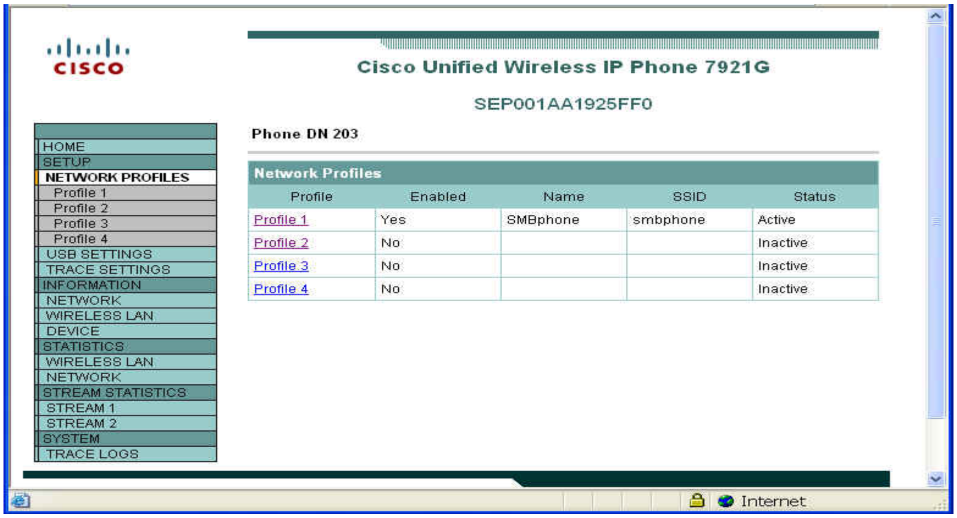
Cisco Unified Wireless IP Phone 7921G

SEP001AA1925FF0

Phone DN 203

WLAN Information	
Active Network Profile	SMBphone
MAC Address	001AA1925FF0
SSID	smbphone
802.11 Mode	802.11b/g
Single Access Point	No
Call Power Save Mode	U-APSD/PS-POLL
BSSID	001aa2fae0f3
Access Point	AP001b.0c92.c77
Tx Power	5 dBm
Channel	1
RSSI	-26
Channel Utilization	242
DTIM period (ms)	102
Security Mode	Auto(AKM)
Encryption	TKIP
Key Management	WPA + CCKM

STEP 4. Configure wireless Profile = Profile1 or make changes to the existing profile as shown below. If the settings are locked – Unlock them by chosing <*><*> and <# >keys. Enter User credentials as configured on the Local Radius Server user=user5 and password=demo. Enable the DHCP server.



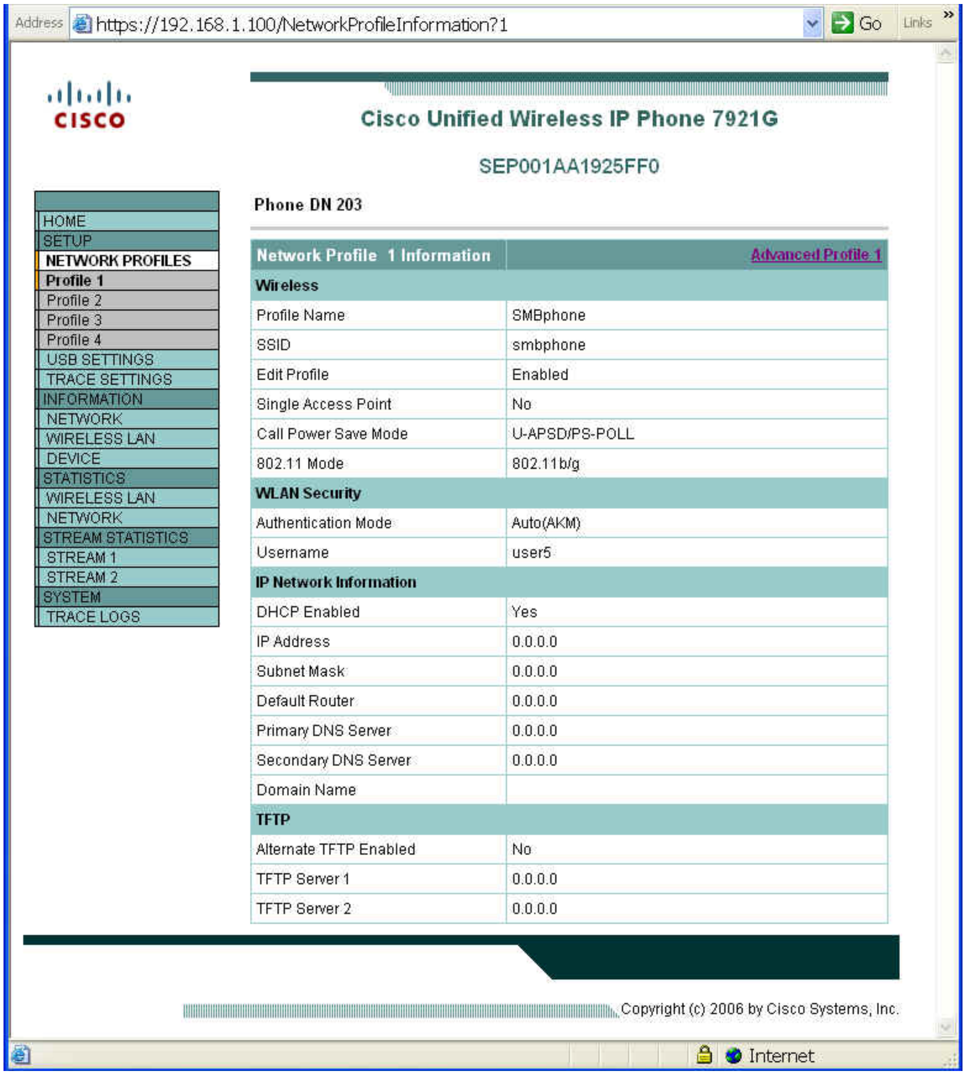
Cisco Unified Wireless IP Phone 7921G

SEP001AA1925FF0

Phone DN 203

Network Profiles

Profile	Enabled	Name	SSID	Status
Profile 1	Yes	SMBphone	smbphone	Active
Profile 2	No			Inactive
Profile 3	No			Inactive
Profile 4	No			Inactive



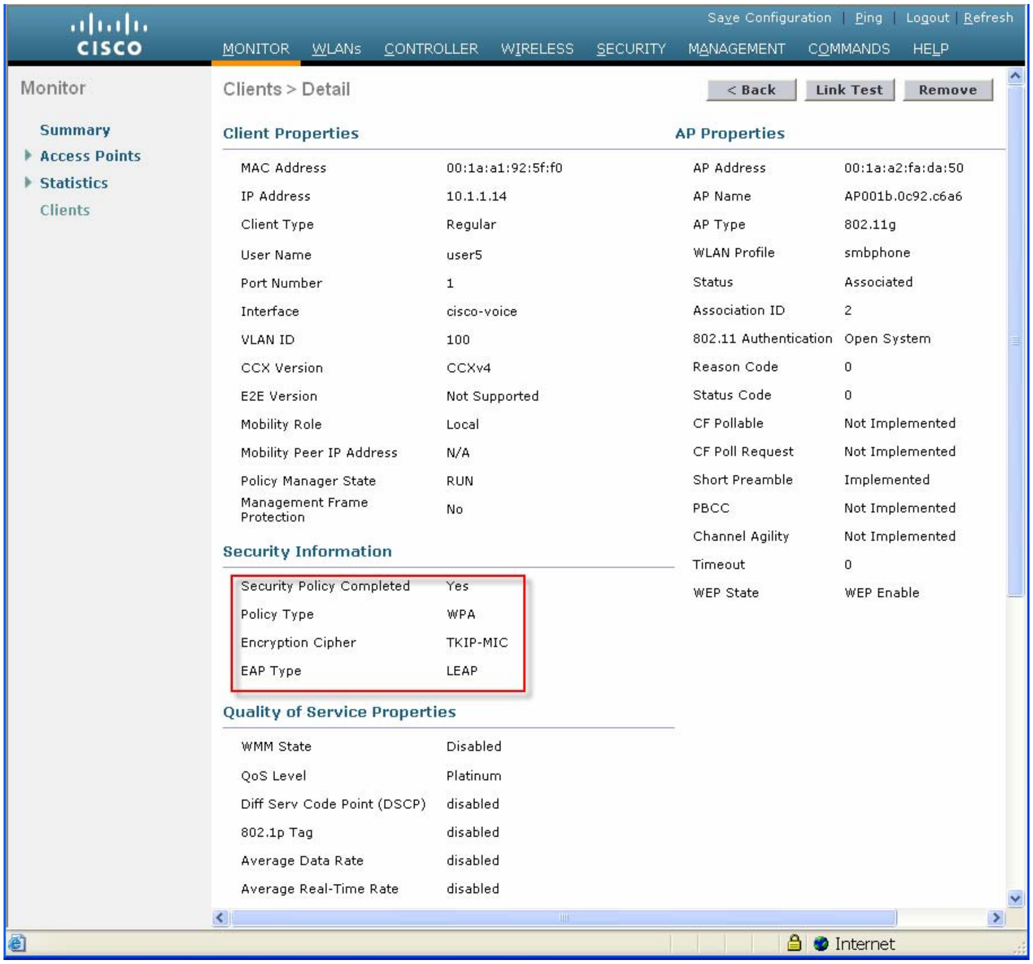
Cisco Unified Wireless IP Phone 7921G

SEP001AA1925FF0

Phone DN 203

Network Profile 1 Information	Advanced Profile 1
Wireless	
Profile Name	SMBphone
SSID	smbphone
Edit Profile	Enabled
Single Access Point	No
Call Power Save Mode	U-APSD/PS-POLL
802.11 Mode	802.11b/g
WLAN Security	
Authentication Mode	Auto(AKM)
Username	user5
IP Network Information	
DHCP Enabled	Yes
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Router	0.0.0.0
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0
Domain Name	
TFTP	
Alternate TFTP Enabled	No
TFTP Server 1	0.0.0.0
TFTP Server 2	0.0.0.0

STEP 5. After configuring the 7921 and connecting to the wireless network verify the phone connectivity authentication and security credentials obtained on the controller Web UI as shown below.


Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Monitor
Summary
Access Points
Statistics
Clients
< Back
Link Test
Remove
Internet

Clients > Detail

Client Properties

MAC Address	00:1a:a1:92:5f:f0
IP Address	10.1.1.14
Client Type	Regular
User Name	user5
Port Number	1
Interface	cisco-voice
VLAN ID	100
CCX Version	CCXv4
E2E Version	Not Supported
Mobility Role	Local
Mobility Peer IP Address	N/A
Policy Manager State	RUN
Management Frame Protection	No

AP Properties

AP Address	00:1a:a2:fa:da:50
AP Name	AP001b.0c92.c6a6
AP Type	802.11g
WLAN Profile	smbphone
Status	Associated
Association ID	2
802.11 Authentication	Open System
Reason Code	0
Status Code	0
CF Pollable	Not Implemented
CF Poll Request	Not Implemented
Short Preamble	Implemented
PBCC	Not Implemented
Channel Agility	Not Implemented
Timeout	0
WEP State	WEP Enable

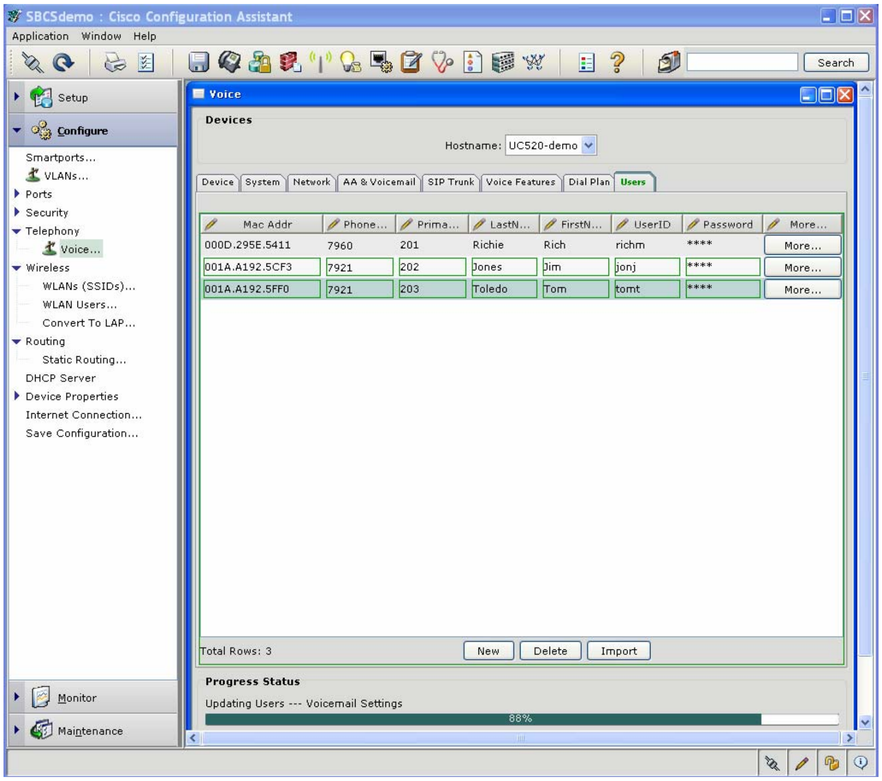
Security Information

Security Policy Completed	Yes
Policy Type	WPA
Encryption Cipher	TKIP-MIC
EAP Type	LEAP

Quality of Service Properties

WMM State	Disabled
QoS Level	Platinum
Diff Serv Code Point (DSCP)	disabled
802.1p Tag	disabled
Average Data Rate	disabled
Average Real-Time Rate	disabled

STEP 6. Verify Phone connectivity to the CME in the CCA as shown below.



Hostname: UC520-demo

Mac Addr	Phone...	Prima...	LastN...	FirstN...	UserID	Password	More...
000D.295E.5411	7960	201	Richie	Rich	richm	****	More...
001A.A192.5CF3	7921	202	Jones	Jim	jonj	****	More...
001A.A192.5FF0	7921	203	Toledo	Tom	tomt	****	More...

Total Rows: 3

Updating Users --- Voicemail Settings

88%

STEP 7. After all the connectivity is verified you should be able to demonstrate the functionality of the 7921 by making calls to a Desktop 7960 phone and other phones if available. Phones extensions examples are shown in the figure above.

Note **7921 clients should be freely moving (roaming) around the demonstration room and observe no latency in the communications since Fast Secure Roaming (CCKM) was configured on the 7921. The 7921 phone will be auto configured in the Voice system. You may want to add names to extensions as you wish.**

Client Failover

STEP 1. Place a call from the 7920 Wireless IP Phone to the 7960.

STEP 2. Answer the call on the 7960 and put the call on mute.

STEP 3. Note which AP the 7920 is associated by looking for a fast blinking Ethernet activity light on the AP. Or you can look in the WLAN Controller or CCA

STEP 4. Disconnect the Ethernet cable from this AP. Talk into the 7920 while doing the demo.

STEP 5. Notice that the phone call will stay active and only takes a second to failover to another AP. The voice interruption should be very minimal.

STEP 6. Verify 7921 phone connection in the Topology View.

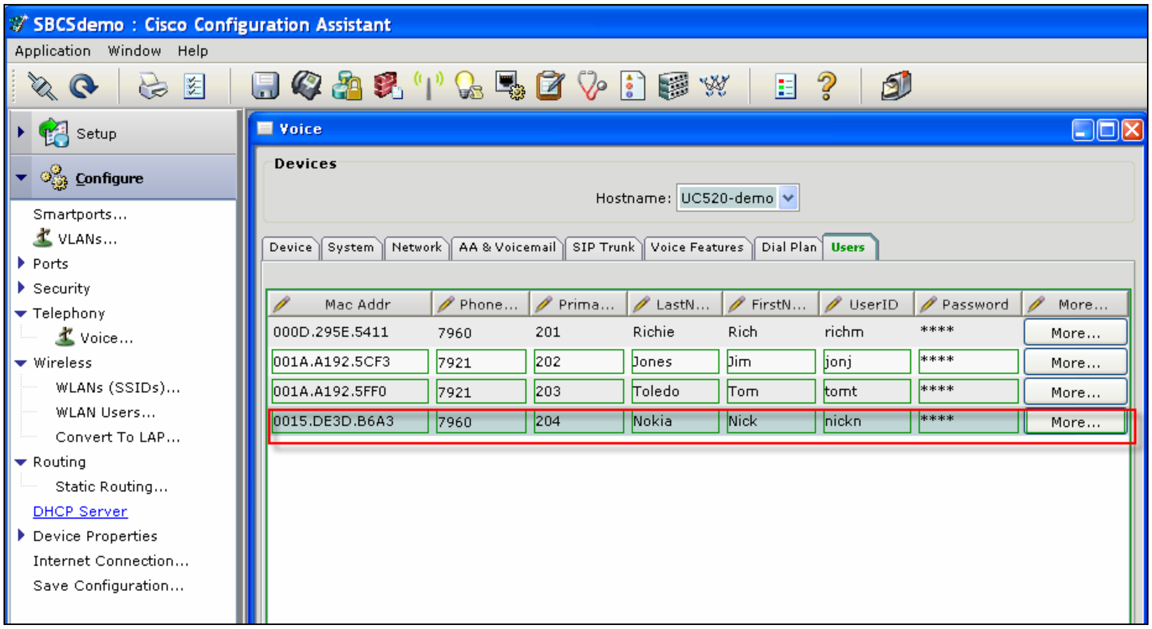
Wireless connectivity with WLC526 LAP521 - Secure connectivity using Wireless Nokia Dual-Mode Phone

Next we can demonstrate setup with WPA/TKIP and 802.1x with Wireless Phone clients. We will initially configure the Nokia device with the GUI interface on the phone supplicant that comes native on the Nokia interface.

STEP 1. We will demonstrate Wireless client connectivity with WPA/PSK on the Nokia wireless phone, but prior to that we will have to setup the Call manager Express with the MAC address of the Nokia E-60-1 dual mode phone.

Note As shown in the figure below the Nokia dual mode phone is setup in the CME as a 7960 desktop phone

---

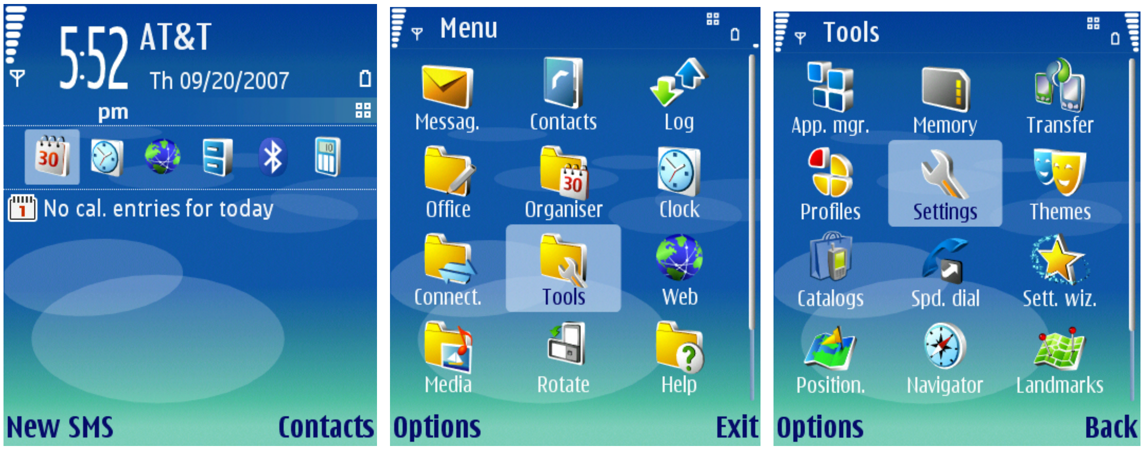


Hostname: UC520-demo

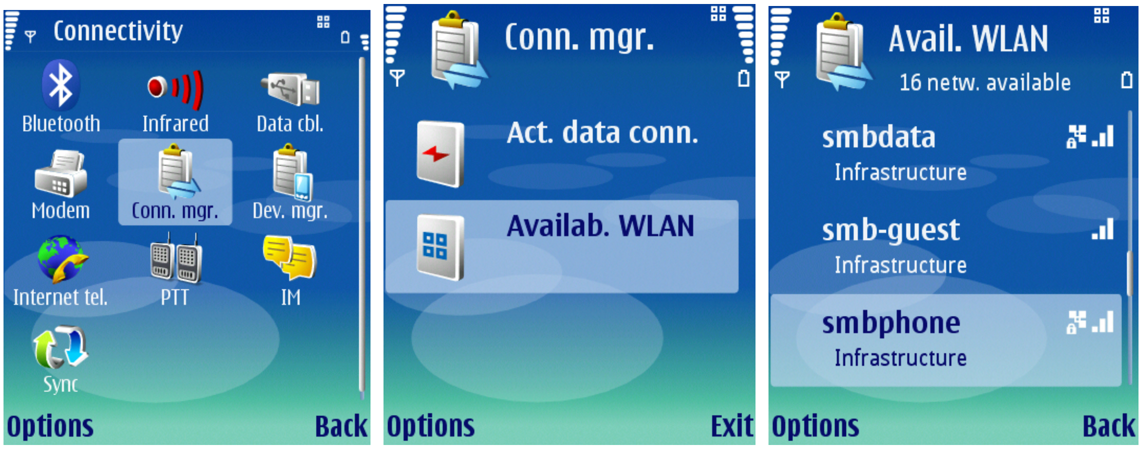
Mac Addr	Phone...	Prima...	LastN...	FirstN...	UserID	Password	More...
000D.295E.5411	7960	201	Richie	Rich	richm	****	More...
001A.A192.5CF3	7921	202	Jones	Jim	jonj	****	More...
001A.A192.5FF0	7921	203	Toledo	Tom	tomt	****	More...
0015.DE3D.B6A3	7960	204	Nokia	Nick	nickn	****	More...

Note : to get serial number of the Nokia phone and other setting you have to start **Intellisynch** in the **Installat**. folder

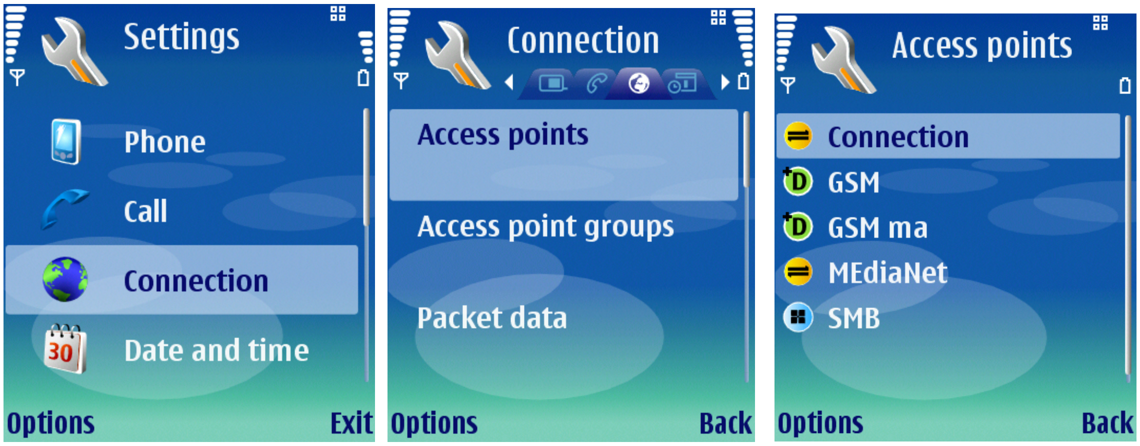
STEP 2. Start configuration of the Nokia phone by pressing the Menu button right below the Navigation Button in the middle and then choose the Tools Icon > Settings.



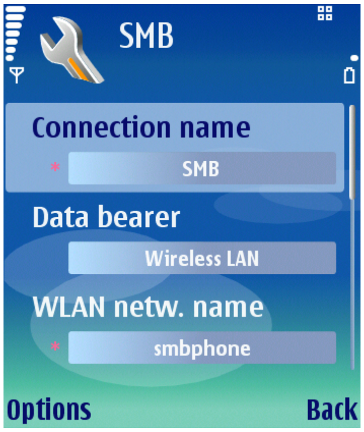
STEP 3. Under the Connectivity Options > Connection Mgr > Available WLAN – find available WLANs seen by the Nokia Dual Mode wireless phone.



STEP 4. Select under the Settings Menu a Connection configuration option for the Access Point and Create or Modify the SMB profile for the Nokia WLAN.



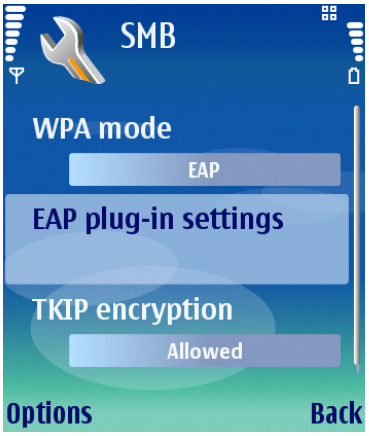
STEP 5. Configure SMB profile for WPA/WPA2 with TKP for Authentication and Encryption and **WLAN=smbphone**, just like on the WLC. Also choose the “EAP plug-in setting” and configure it for LEAP at the highest priority and also configure under the LEAP settings User Credentials **User=user5, Password=demo**


SMB

Connection name
* SMB

Data bearer
Wireless LAN

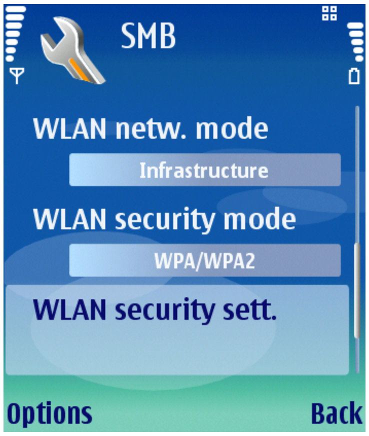
WLAN netw. name
* smbphone


SMB

WPA mode
EAP

EAP plug-in settings

TKIP encryption
Allowed

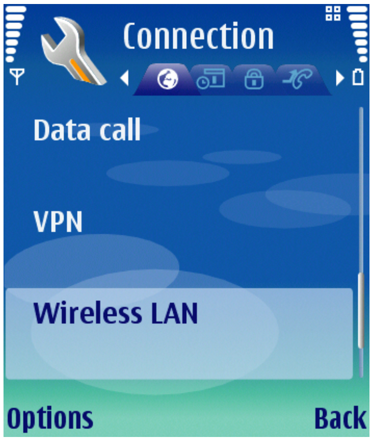

SMB

WLAN netw. mode
Infrastructure

WLAN security mode
WPA/WPA2

WLAN security sett.

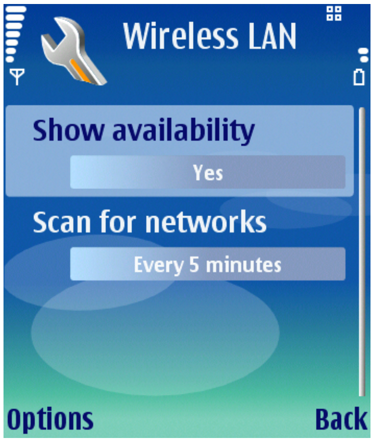
STEP 6. Setup the Wireless LAN connection and then the SMB profile under the Access


Connection

Data call

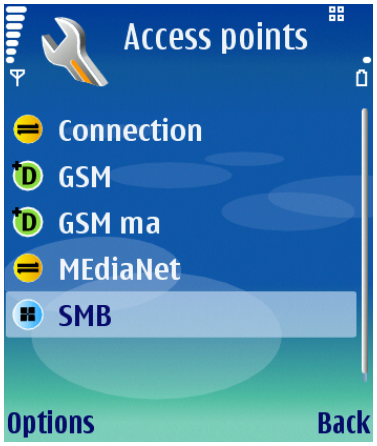
VPN

Wireless LAN


Wireless LAN

Show availability
Yes

Scan for networks
Every 5 minutes


Access points

Connection

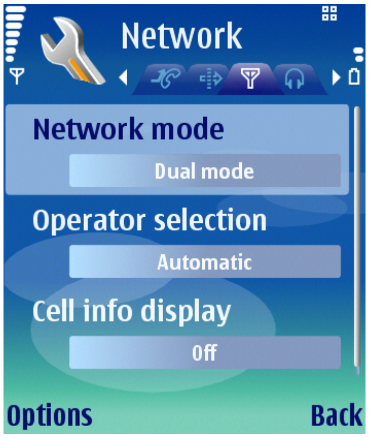
GSM

GSM ma

MEdiaNet

SMB

STEP 7. Select Dual Mode operation, verify SCCP configuration for CME connection and Voice Profile.



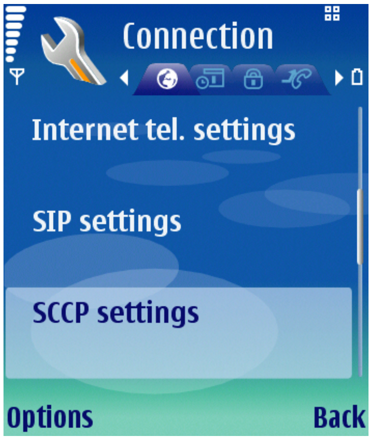
Network

Network mode
Dual mode

Operator selection
Automatic

Cell info display
Off

Options Back



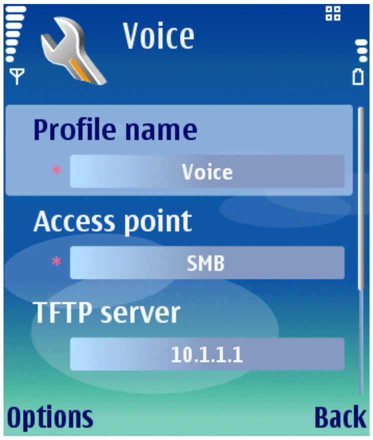
Connection

Internet tel. settings

SIP settings

SCCP settings

Options Back



Voice

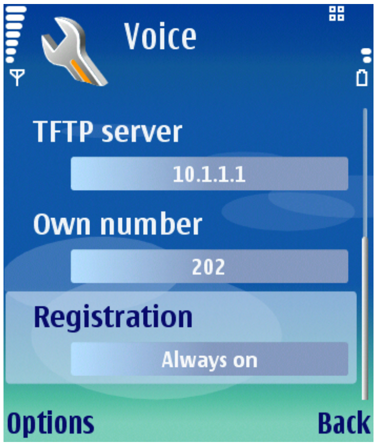
Profile name
* Voice

Access point
* SMB

TFTP server
10.1.1.1

Options Back

STEP 8. After successful Authentication the Nokia dual mode phone will receive CME extension and the call can be places to the Desktop phone extension 201.



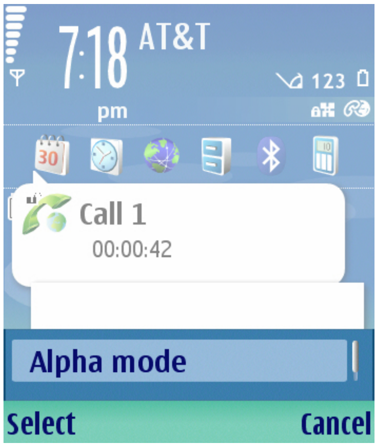
Voice

TFTP server
10.1.1.1

Own number
202

Registration
Always on

Options Back



7:18 pm AT&T
123

Call 1
00:00:42

Alpha mode

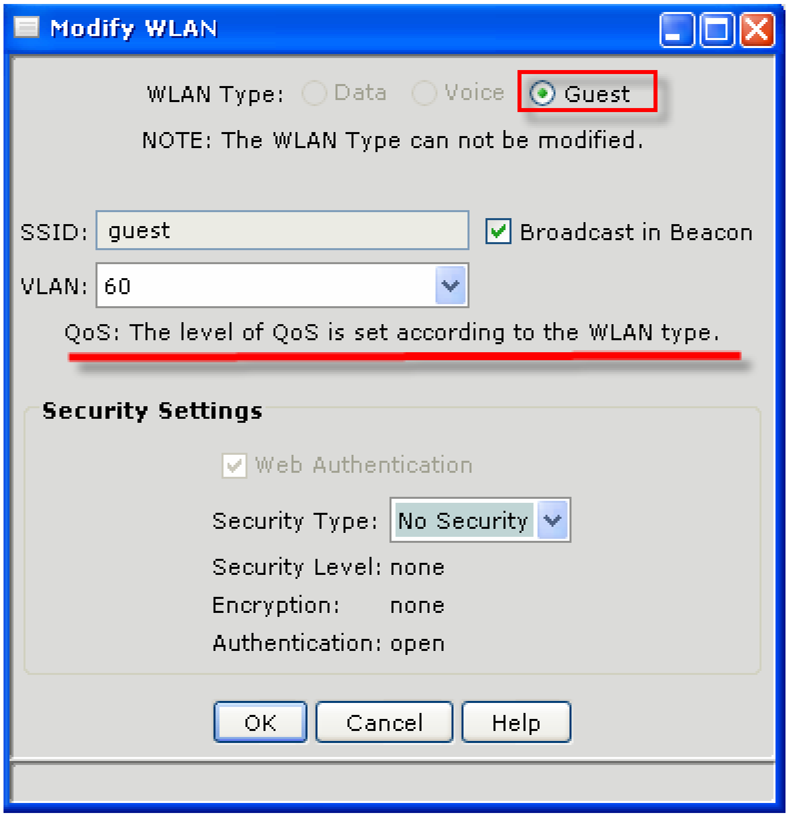
Select Cancel

Note Please note in the Figure above when Phone is connected to the CME and has extension there is a little Icon right below the Battery Icon. Also note that when phone is connected to the WLAN (primary wireless connection) the Little Clover icon with the Lock right below the 123.

Create Guest Web Authentication

In the Present release code of the CCA version 1.6 the Guest Access is configurable now right via the CCA interface.

STEP 8. Create Guest User interface in the CCA prior to configuring Guest SSID. Under **Wireless> WLANs…>** in CCA. For Guest User we create VLAN 60 with no security.



Modify WLAN

WLAN Type: ○ Data ○ Voice ● Guest

NOTE: The WLAN Type can not be modified.

SSID: guest ☑ Broadcast in Beacon

VLAN: 60

QoS: The level of QoS is set according to the WLAN type.

Security Settings

☑ Web Authentication

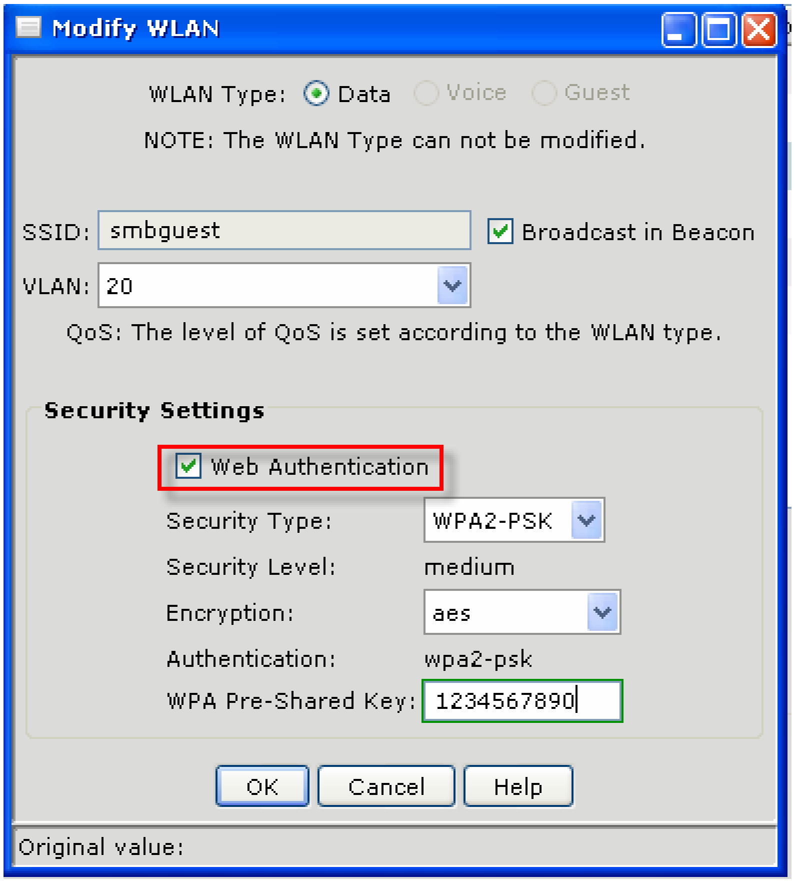
Security Type: No Security

Security Level: none

Encryption: none

Authentication: open

STEP 9. From the same interface create another WLAN = smbguest , this time on VLAN 20 with Web Authentication checked and security set WPA2-PSK /AES



Modify WLAN

WLAN Type: ● Data ○ Voice ○ Guest

NOTE: The WLAN Type can not be modified.

SSID: smbguest ☑ Broadcast in Beacon

VLAN: 20

QoS: The level of QoS is set according to the WLAN type.

Security Settings

☑ Web Authentication

Security Type: WPA2-PSK

Security Level: medium

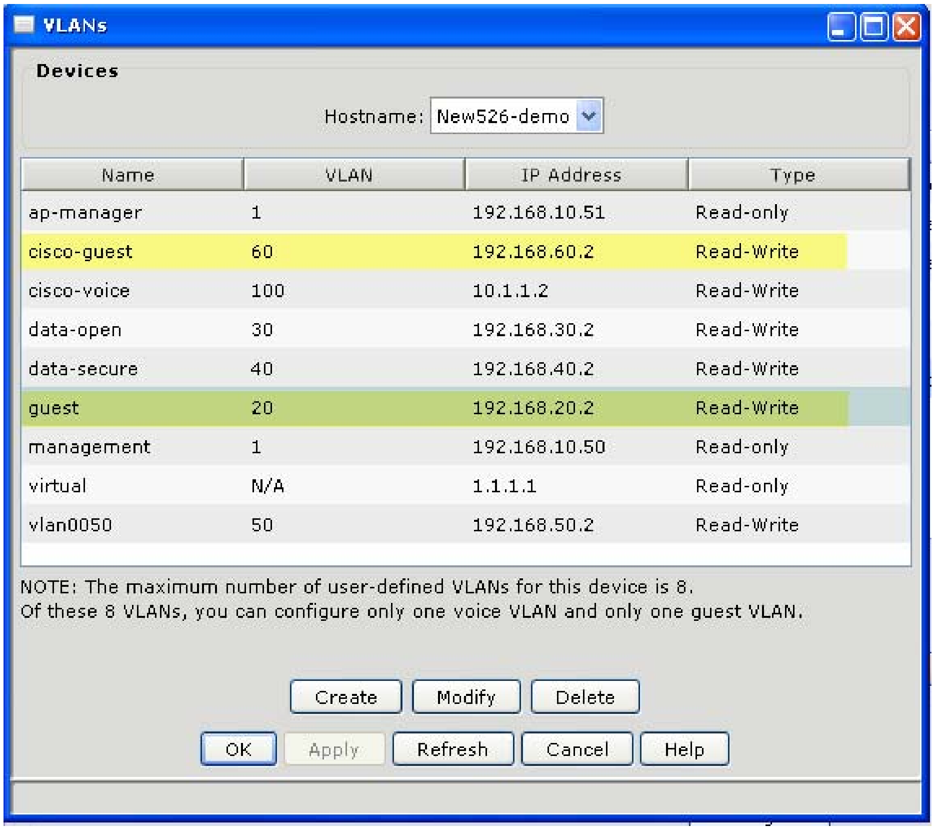
Encryption: aes

Authentication: wpa2-psk

WPA Pre-Shared Key: 1234567890

Original value:

STEP 10. Configure the IP address of the Interface “guest’ and “smbguest” , Subnet Mask, Default Gateway and DHCP server as shown below.

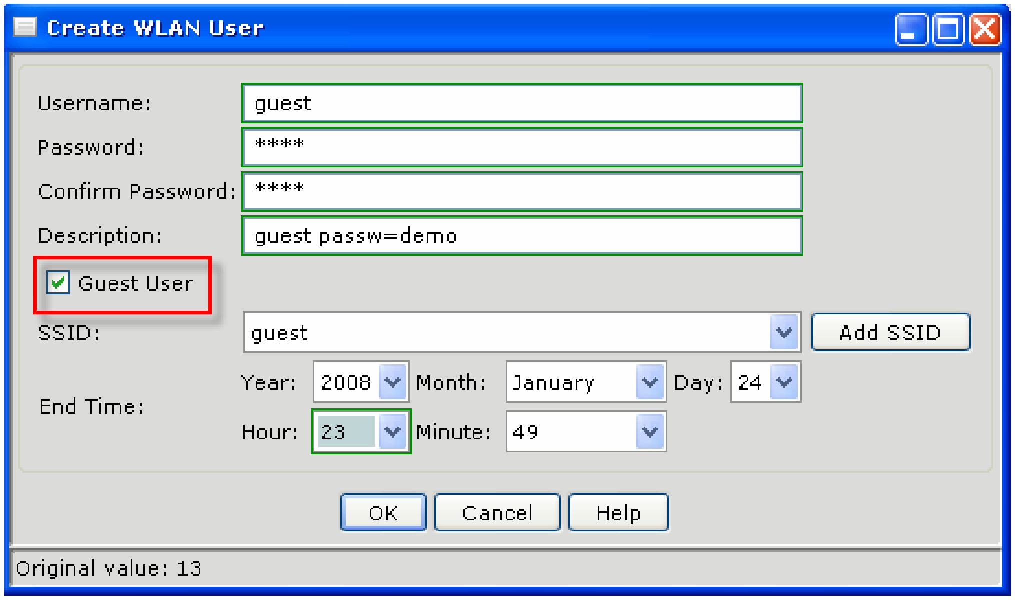


Hostname: New526-demo

Name	VLAN	IP Address	Type
ap-manager	1	192.168.10.51	Read-only
cisco-guest	60	192.168.60.2	Read-Write
cisco-voice	100	10.1.1.2	Read-Write
data-open	30	192.168.30.2	Read-Write
data-secure	40	192.168.40.2	Read-Write
guest	20	192.168.20.2	Read-Write
management	1	192.168.10.50	Read-only
virtual	N/A	1.1.1.1	Read-only
vlan0050	50	192.168.50.2	Read-Write

NOTE: The maximum number of user-defined VLANs for this device is 8.
Of these 8 VLANs, you can configure only one voice VLAN and only one guest VLAN.

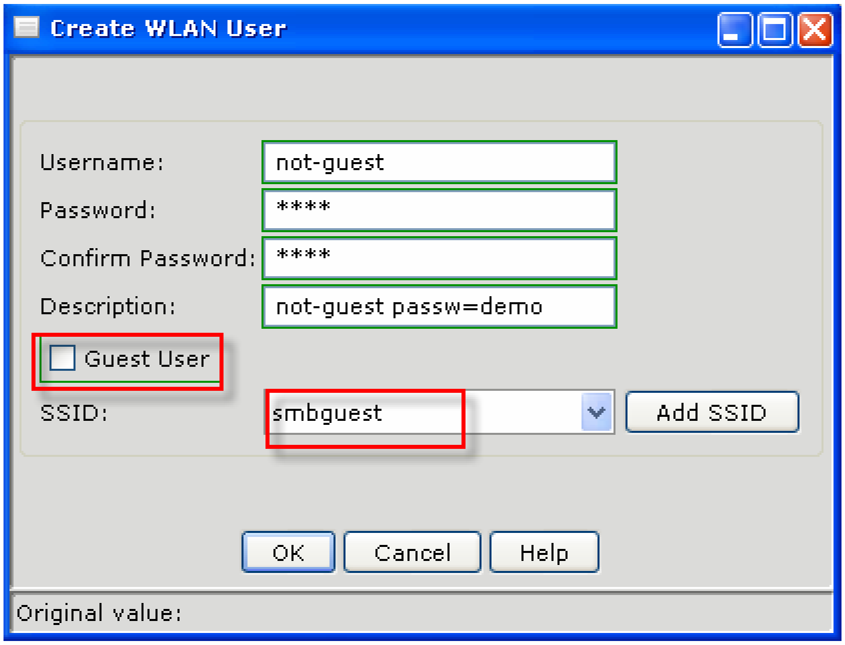
STEP 11. After SSID “guest” was created in the CCA 1.6 Configure>Wireless> WLAN Users…> create new user guest as shown below. Note when creating user guest there are options available in this release that allow you to configure the times guest user is permitted on the network.



Username: guest
Password: ****
Confirm Password: ****
Description: guest passw=demo
☑ Guest User
SSID: guest
End Time: Year: 2008 Month: January Day: 24
Hour: 23 Minute: 49

Original value: 13

STEP 12. Under the same screen create another Guest user “smbguest” but this time don’t check the Guest User box; this setup will allow you to map the not-guest user to a smbguest SSID that has different security credentials. This is a very useful setup when a “not-guest” users can be connected to the wireless network using Web-auth credentials and without and AAA server.



Create WLAN User

Username: not-guest

Password: ****

Confirm Password: ****

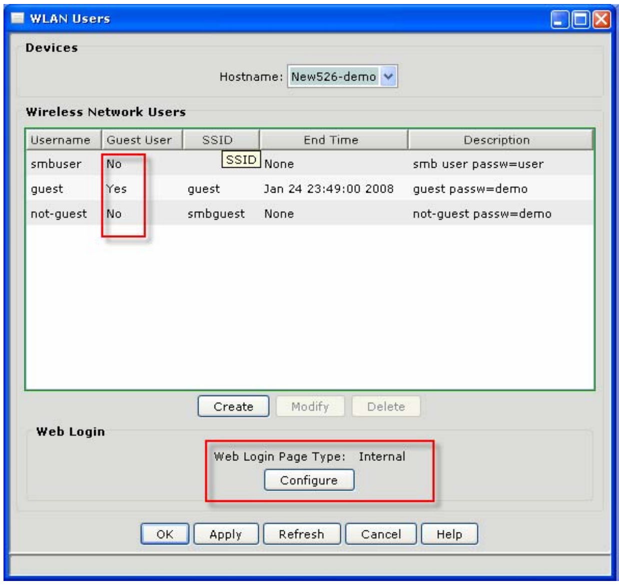
Description: not-guest passw=demo

□ Guest User

SSID: smbguest

Original value:

STEP 1. From the same tab <WLAN Users…> you can create or modify the Web Authentication page as shown below.



WLAN Users

Devices

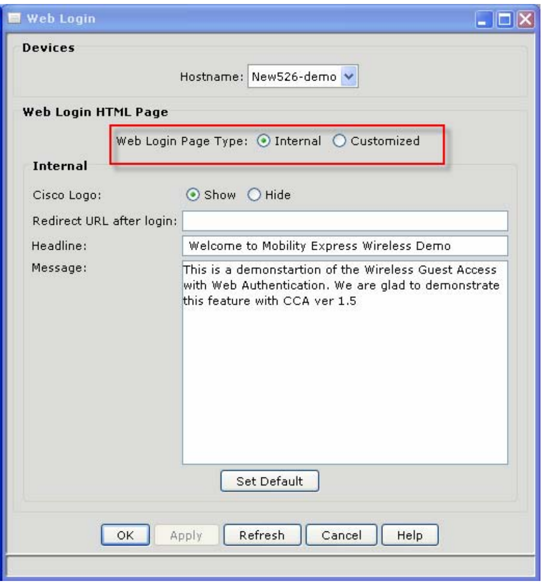
Hostname: New526-demo

Wireless Network Users

Username	Guest User	SSID	End Time	Description
smbuser	No		None	smb user passw=user
guest	Yes	guest	Jan 24 23:49:00 2008	guest passw=demo
not-guest	No	smbguest	None	not-guest passw=demo

Web Login

Web Login Page Type: Internal



Web Login

Devices

Hostname: New526-demo

Web Login HTML Page

Web Login Page Type: ● Internal ○ Customized

Internal

Cisco Logo: ● Show ○ Hide

Redirect URL after login:

Headline: Welcome to Mobility Express Wireless Demo

Message: This is a demonstartion of the Wireless Guest Access with Web Authentication. We are glad to demonstrate this feature with CCA ver 1.5

Note Lobby ambassador from the Web UI or System administrator has to create all the Guest and Local Net user accounts. Also note that session timeout will impact the Lifetime of the local net user. The session will end whatever ends sooner the Lifetime or the session timeout timer. Session timeout of "0" means session for that WLAN will not expire.

STEP 2. Click **Hide or Show** if you want Cisco Logo to appear on the log on page.

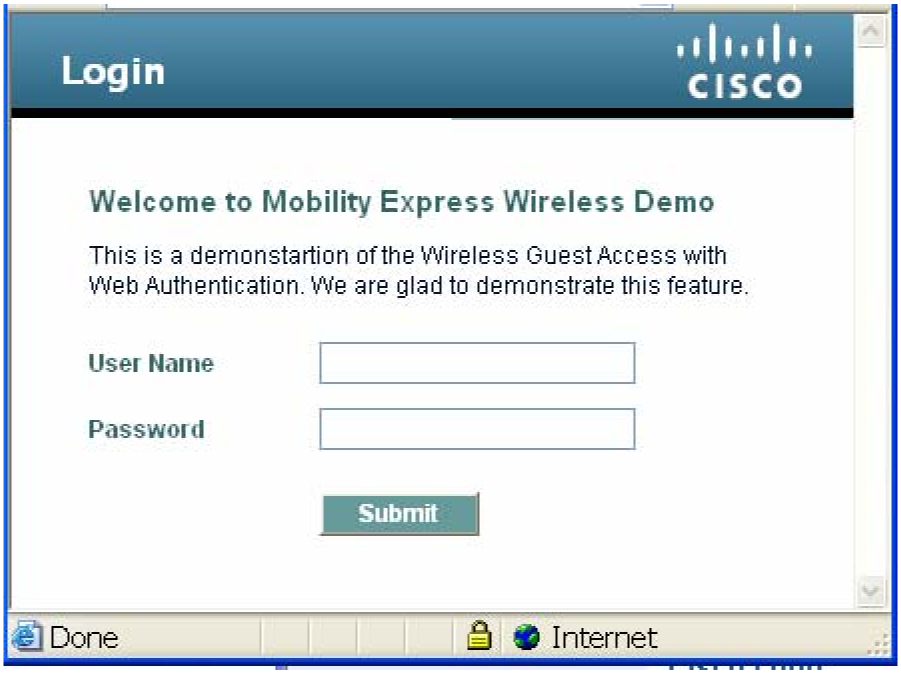
STEP 3. To direct user to another specific URL (such as your company URL) after login, enter the www.companyname.com URL up to 254 characters.

STEP 4. Enter information (up to 127 characters) in the Headline field. Default is "Welcome to Cisco Wireless Network"

STEP 5. To display message in the Web Login page, enter desired text up to 2047 characters. Example shown above.

STEP 6. Click **Apply** to save changes. Save configuration on the controller.

STEP 7. You can preview the login page by clicking on Preview



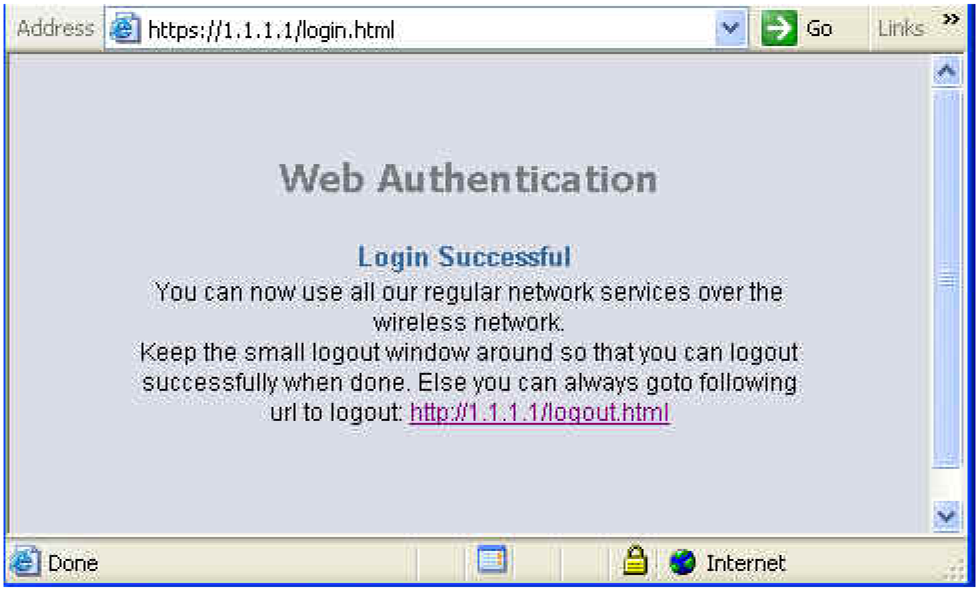
Welcome to Mobility Express Wireless Demo

This is a demonstartion of the Wireless Guest Access with Web Authentication. We are glad to demonstrate this feature.

Note You must Save configuration and reboot the 526 controller to commit the changes. To Reload the controller in CCA choose **Maintenance** > **Restart/Reset…**

STEP 8. Login to the WLAN Controller web authentication screen using "guest/guest"

STEP 9. Verify that client is able to freely use all network functions by reentering the reachable HTTP site address.



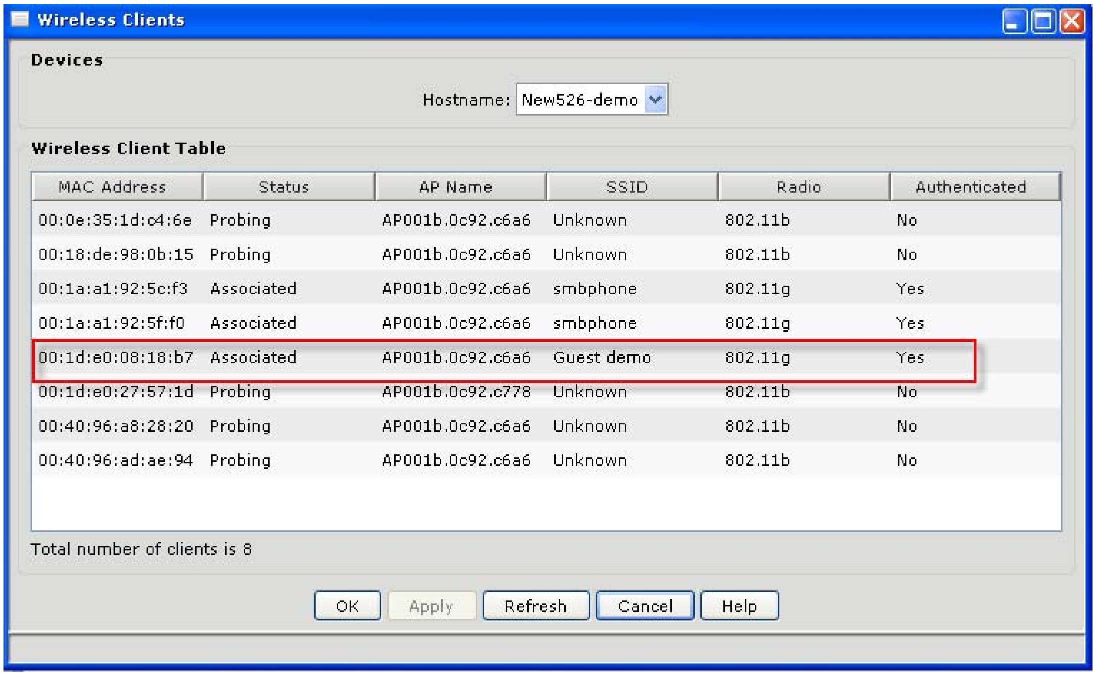
Web Authentication

Login Successful

You can now use all our regular network services over the wireless network.
Keep the small logout window around so that you can logout successfully when done. Else you can always goto following url to logout: http://1.1.1.1/logout.html

STEP 10. Verify that client appears on the WLAN Controller' client list as Associated and Authenticated.

STEP 11. Click on the **Monitor** > **Report** > **Wireless Client** link to view associated client detail table. Guest clients should show as associated in the table with configured **Guest** profile.



Devices

Hostname: New526-demo

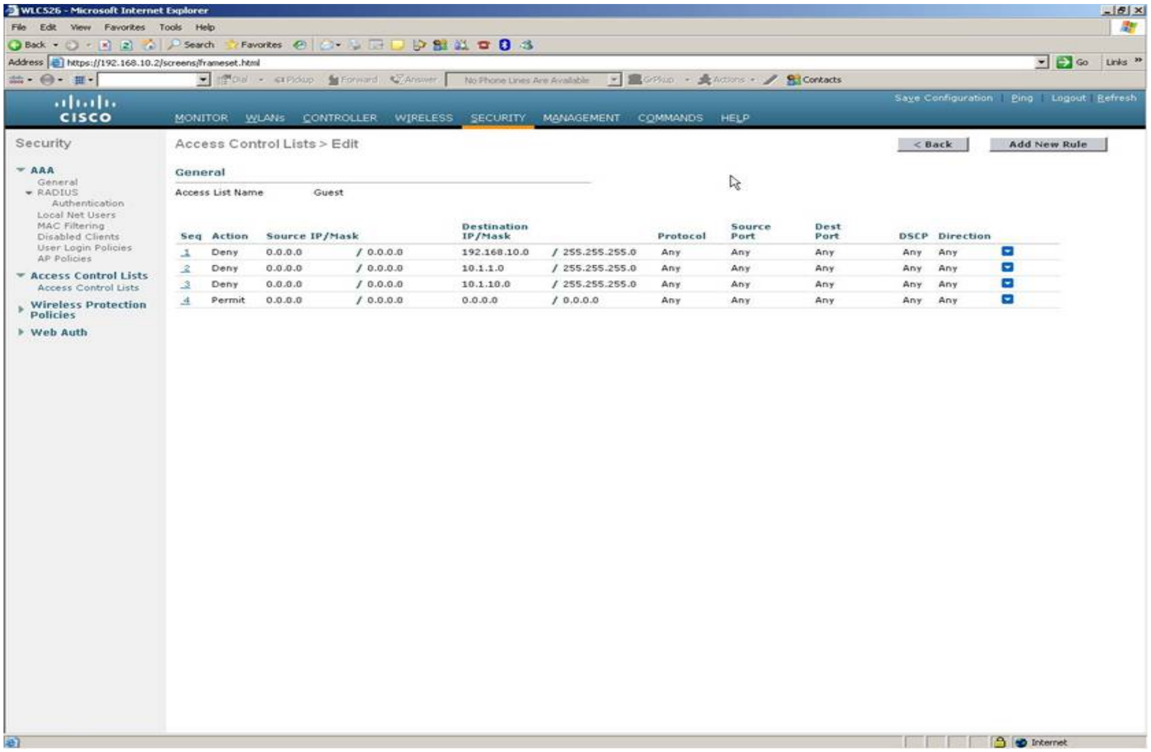
Wireless Client Table

MAC Address	Status	AP Name	SSID	Radio	Authenticated
00:0e:35:1d:c4:6e	Probing	AP001b.0c92.c6a6	Unknown	802.11b	No
00:18:de:98:0b:15	Probing	AP001b.0c92.c6a6	Unknown	802.11b	No
00:1a:a1:92:5c:f3	Associated	AP001b.0c92.c6a6	smbphone	802.11g	Yes
00:1a:a1:92:5f:f0	Associated	AP001b.0c92.c6a6	smbphone	802.11g	Yes
00:1d:e0:08:18:b7	Associated	AP001b.0c92.c6a6	Guest demo	802.11g	Yes
00:1d:e0:27:57:1d	Probing	AP001b.0c92.c778	Unknown	802.11b	No
00:40:96:a8:28:20	Probing	AP001b.0c92.c6a6	Unknown	802.11b	No
00:40:96:ad:ae:94	Probing	AP001b.0c92.c6a6	Unknown	802.11b	No

Total number of clients is 8

Note When setting up a guest VLANs, there is no separation applied between the VLANs in this release, meaning that if guest user logs on through your controller it can access any subnet in use on the UC500, if one is implemented on your network (e.g. your data vlan, voice vlan, etc….) by connecting to the guest network's default gateway.

The work around in this release of CCA 1.0 - 1.6 is to apply ACL's on the UC500 or on the 526 controller. Create the ACLs on the controller as shown in the example below:


WLC526 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address https://192.168.10.2/screens/frameset.html
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Save Configuration | Ping | Logout | Refresh
Security
AAA
General
RADIUS
Authentication
Local Net Users
MAC Filtering
Disabled Clients
User Login Policies
AP Policies
Access Control Lists
Access Control Lists
Wireless Protection Policies
Web Auth
< Back
Add New Rule

Access Control Lists > Edit

General

Access List Name Guest

Seq	Action	Source IP/Mask		Destination IP/Mask		Protocol	Source Port	Dest Port	DSCP	Direction
1	Deny	0.0.0.0	/ 0.0.0.0	192.168.10.0	/ 255.255.255.0	Any	Any	Any	Any	Any
2	Deny	0.0.0.0	/ 0.0.0.0	10.1.1.0	/ 255.255.255.0	Any	Any	Any	Any	Any
3	Deny	0.0.0.0	/ 0.0.0.0	10.1.10.0	/ 255.255.255.0	Any	Any	Any	Any	Any
4	Permit	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any	Any	Any

Web Authentication lockout

STEP 1. Start WWW browser on SE Laptop and browse to **https:// 1.1.1.1/login.html** .You will get a redirect to the web authentication page

STEP 2. At the WebAuth login screen, login using the “guest” User Name however, use an incorrect password 4 times.

STEP 3. After the fourth try, you will you will not be able to login.

STEP 4. In WLC Web UI interface go to **Monitor** mode and in **Client Summary** you should see **Excluded Clients**.

STEP 5. Within 20 seconds, the SE Laptop will not be associated with the AP.

STEP 6. From the **MONITOR** > **Wireless Clients**, remove the client from the Excluded list. Remove this client by choosing **Remove** in the Command drop down box.

STEP 7. Start WWW browser on SE Laptop or PDA , and the WebAuth login screen should appear and clients should be able to login as Guest user

STEP 8. Lastly you can create a user as “Lobby Administrator” that has rights to create guest users only on the Controller. Lobby Administrator would need access to the Controller WebUI interface to create guest users with scheduled network access.

APPENDIX-A — IP ADDRESSING AND ACCOUNT INFORMATION

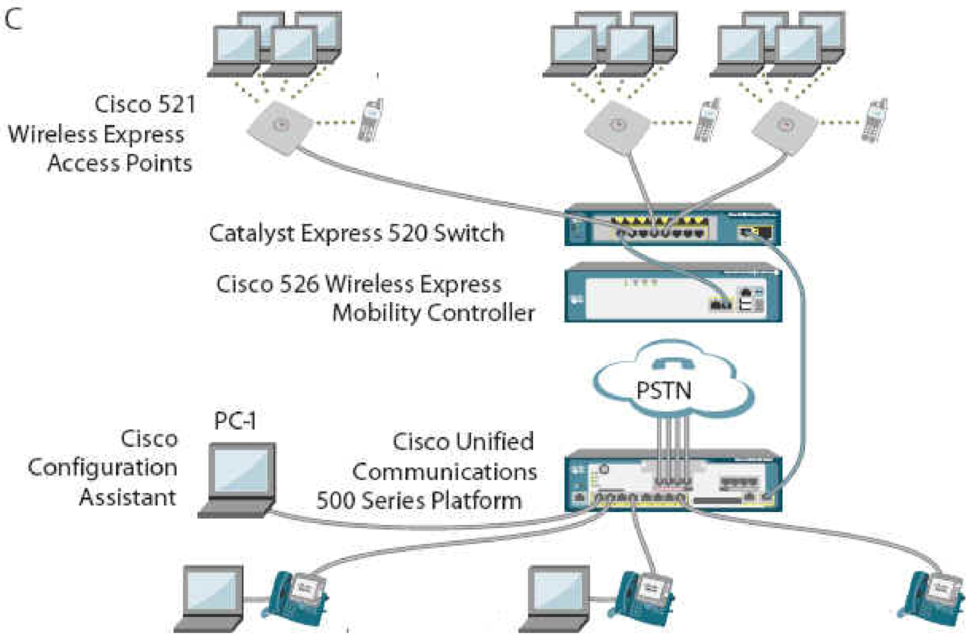

C
Cisco 521 Wireless Express Access Points
Catalyst Express 520 Switch
Cisco 526 Wireless Express Mobility Controller
PSTN
PC-1
Cisco Configuration Assistant
Cisco Unified Communications 500 Series Platform

Table 1. Device Management Access

Device	IP Address	User	Password
Laptop	192.168.20.X (Guest User)	NA	NA
Cisco 521 AP	Created during the demo	NA	NA
Cisco UC520	192.168.10.1	admin	cisco
526 WLAN Controller	192.168.10.50 (Management Interface)	admin	cisco
Local RADIUS server	192.168.10.1	n/a	Key=demo

Table 2. Cables

Cables	UC 520	Device end	Quantity
6'– Cat 5e Patch Cable	Fa 0	7960 IP Phone	1 or 2
6'– Cat 5e Patch Cable	Fa 1, 2	Laptop	2
6'– Cat 5e Patch Cable	Fa 3,4,5	521 LAP	3
6'– Cat 5e Patch Cable	Fa 6		1
6'– Cat 5e Patch Cable	Fa 7	WLC 526	1
6'– Cat 5e Patch Cable - optional	Exp	CE 520	1

Cables	UC 520	Device end	Quantity
6' – Console Cable - optional	Console Port		1

Table 3. Wireless LAN SSIDs

Description	IP address	Username	Password
SSID: dataopen (EAP/802.1x)	192.168.30.1	n/a	n/a
SSID : datasec (WPA2/AES/802.1X)	192.168.40.1	n/a	n/a
SSID: smbguest (WPA2-PSK/AES/WEBAUTH)	192.168.20.1	Not-guest	demo
SSID: smbphone (WPA/TKIP/802.1X-CCKM)	10.1.1.1	n/a	n/a
SSID: voice (open)	10.1.1.1	n/a	n/a
**** SSID: smbdata (WPA-PSK/TKIP/WEBAUTH)**	192.168.50.1	n/a	WPA PS key=sbcsdata
**** SSID: guest (web authentication)**	192.168.60.1	guest	guest

**Created during the demo

Table 4. Wireless Users

User ID	Password	Description
User1	demo	Wireless user
User2	demo	Wireless user
User3	demo	Wireless user
User4	demo	Wireless user
Guest	demo	guest
Not-Guest	demo	Not-guest

Table 5. Voice

Extension	IP address	Description
Mobility ExpressCallManager Express	10.0.5.254/ccme.html	admin/cisco123
201	10.0.X.X	7960 IP Phone
202	10.0.X.X	7920 IP Phone
205	10.0.X.X	IP Communicator

APPENDIX-B — CISCO CONFIGURATION ASSISTANT 1.6

Cisco Configuration Assistant, a PC-based intuitive GUI configuration tool, is an integral component of the Cisco Smart Business Communications System. With a focus on ease of use, the Cisco Configuration Assistant simplifies configuration of multiple technologies-unified communications, switching, routing, security, and wireless. Cisco Configuration Assistant simplifies telephony configuration and provides follow-up support to facilitate easy modification. Features include an interactive topology view, front-panel views of devices, and drag-and-drop Cisco IOS Software upgrades.

Cisco Configuration Assistant was purpose-built to provide comprehensive configuration, deployment, and ongoing network management support for the entire line of products in the Cisco Smart Business Communications System. (For a list of all supported devices and limits, see Table 1.)

Simplified Configuration

A single configuration error in just one device in your network can impede the performance of your essential business applications and leave your business vulnerable to a damaging security breach, so proper device configuration is critical. However, even a small office network can contain a wide range of routing, switching, wireless, and voice solutions. Manually configuring all of them can be a tedious and time-consuming task. Cisco Configuration Assistant reduces the time and effort your IT staff must devote to device configuration by simplifying this process through an easy-to-use GUI. This integrated approach encompasses:

- Voice configuration: To manually configure a Cisco IP telephony system, you would need to configure the Cisco Unified Communications Manager Express call processing and Cisco Unity® Express voicemail applications embedded in your Cisco Integrated Services Router, as well as configure your network routers and switches to support voice communications. Alternatively, Cisco Configuration Assistant can interact with and configure all voice applications and devices dynamically. Simply access the telephony services through the phone icon on the Cisco Configuration Assistant dashboard to easily set up, configure, and apply security to your router and phone system.

- Router configuration: Cisco Configuration Assistant supports router configurations and port settings from LAN and WAN interface configurations. The tool makes it easy to assign IP addresses and subnet masks and change the status of Dynamic Host Configuration Protocol (DHCP), among other capabilities.

- Router security configuration: Cisco Configuration Assistant allows users to activate the most commonly used Cisco IOS® Software security features, including Network Address Translation (NAT), firewalls, and VPNs. The tool guides users to select appropriate parameters that meet the security needs of their network, based on Cisco best practices for network security that have been validated by Cisco network design engineers.

- Switch configuration: Cisco Configuration Assistant provides a quick and easy way to configure ports on switch devices. The tool enables dynamic virtual LAN (VLAN) assignment of voice and data traffic and simplifies activation of quality of service (QoS), security, and Power over Ethernet (PoE) features.

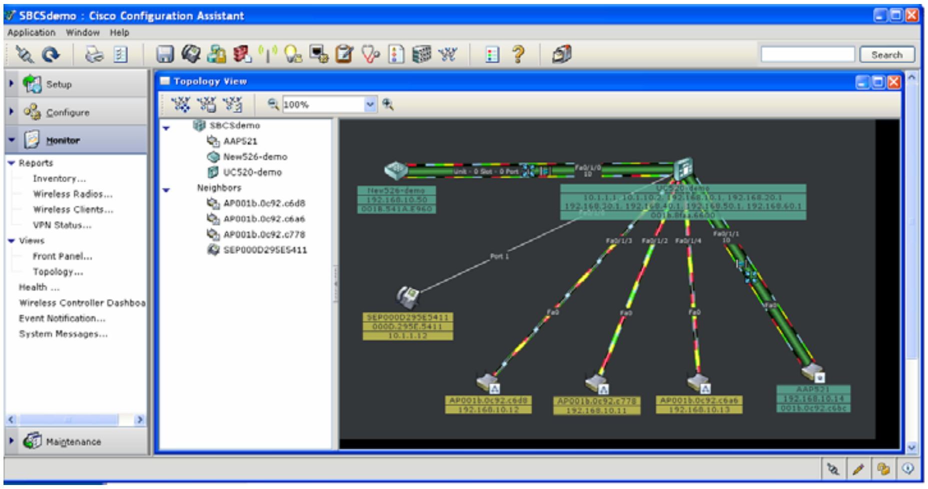
- Wireless configuration: Because airwaves can cross physical security boundaries, proper security on wireless LANs (WLANs) is essential. Cisco Configuration Assistant can configure either a single access point or multiple access point networks. For standalone access points, Cisco Configuration Assistant guides users through the configuration of Secure Set Identifier (SSID), authentication, and encryption. It will also configure multiple access point networks and supports controller-based solutions such as the Cisco Mobility Express solution.

Cisco Configuration Assistant Key Features

Cisco Configuration Assistant provides the following features and benefits:

- Holistic, network-level insight through multiple network views-Users can access devices and monitor the network from two perspectives: the physical Topology View or the Front Panel View. The rich Topology View graphically represents the types of devices in the network as well as detailed information about device status, physical connections, and various monitoring capabilities-all from a single view. The Front Panel View displays all switches and routers in the network simultaneously, along with the state, duplex, and speed of ports. The Front Panel View also allows users to apply features across multiple ports or multiple switches when configuring features such as VLANs. In addition, users can verify optimal ongoing network performance by generating comprehensive, real-time reports of network inventory and health.

Figure 7. The Topology View graphically represents the types of devices in the network and provides detailed information about device status and physical connections



• Simplified topology mapping and deployment through dynamic discovery-Cisco Configuration Assistant's unique discovery capabilities provide users with total control when discovering network devices to create a community. Users can discover devices by entering a seed IP, range IP, subnet IP, or a single IP address. This feature provides more flexibility and time savings when designing the topology.

• Clear separation of services through VLAN highlighting-From the Topology View, users can associate VLAN numbers with colors to quickly view what devices are in a VLAN. Devices that are associated with more than one VLAN display two or more colors with a striped effect.

• Customization with annotated text-Users can add additional text under devices in the Topology View to further describe aspects of the network, such as the name of a building, floor, or closet.

• Improved network visibility with continual health monitoring-Users can quickly assess the status of switches and routers, including packet errors; temperature; PoE status; and bandwidth, CPU, memory, and ternary content addressable memory (TCAM) usage-all from a single window. Users can select the specific health categories to monitor. For each category selected, the switch with the highest usage is displayed in the quick view. Users can access a more comprehensive view by clicking the "Details" button.

• Simplified network reporting-Users can print easy to read reports such as bandwidth utilization. The enhanced print option even allows users to print the Topology View or Front Panel View on one page using the "fit to page" option.

• Enhanced security for configuration and monitoring activities-Cisco Configuration Assistant provides a secure connection between the Cisco Configuration Assistant client and each connected device in the network to safeguard all sensitive information.

• Increased IT staff efficiency through simplified software updates-The drag-and-drop Cisco IOS Software Upgrade feature simplifies the process of upgrading the Cisco IOS Software on a Cisco Catalyst® switch or Cisco router or access point. Users can download the latest software version by simply dragging the update's icon from the PC desktop and dropping it onto the icon of the target device depicted in the Topology View. This process eliminates the need to use the specific Cisco IOS Software filename or select a specific Trivial File Transfer Protocol (TFTP) server IP address when performing updates. This process can also be use to deploy Cisco Unified Express images, phone loads, music on hold files and language packs onto the router.

• Improved network security and performance with dynamic application updates-Users can stay up-to-date on the latest versions and security patches of Cisco Configuration Assistant through dynamic application updates. With this function, users can be assured that when a newly purchased Cisco device is added to the network, it is automatically supported and secured with the latest update.

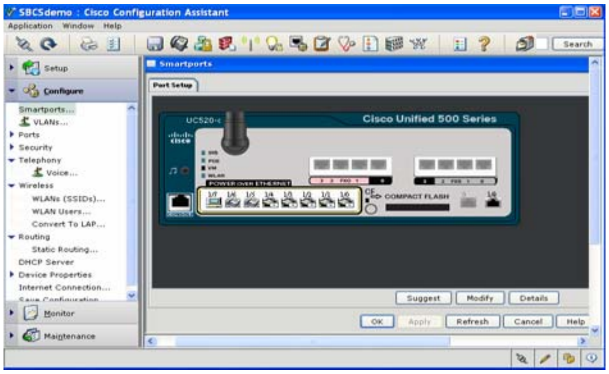
• Enhanced ability to identify and address issues-The Event Notification feature alerts users if a potential problem arises with a device in the network, if a configuration change is required, or if a new version of Cisco Configuration Assistant is available for download. A dialog box provides all necessary information regarding the event, including time; description; and, if applicable, suggestions to resolve the problem.

• Enhanced productivity of partners and guests-Cisco Configuration Assistant's Guest Port feature allows businesses to easily configure guest access ports on their switch, providing visiting guests with Internet access and allowing them to establish VPN connectivity to their company resources. Guest Port users are separated from internal network traffic so that confidential "internal access only" information and services remain secure from unauthorized guest users.

- Increased security and performance through network synchronization-This feature detects inconsistent settings in the network such as VLAN mismatches, centralized time, and security policies. Working with the Troubleshooting Advisor, users can detect and fix these inconsistencies easily.
- Simplified troubleshooting-Embedded in the application is the Troubleshooting Advisor, which simplifies troubleshooting by automatically identifying potential network problems and documenting them with a graphical trend chart. Examples include cabling problems, configuration errors, and other potential network problems. Users receive an explanation of the issue and often can correct the problem with a simple mouse click.
- Enhanced IT staff effectiveness through comprehensive online support-A detailed, transparent help function embedded in Cisco Configuration Assistant provides an extensive glossary and powerful search engine that help users quickly and easily find the information they need to apply specific settings. With these online help features, users often can troubleshoot and resolve problems without having to call for technical support.
- Faster network configuration and improved network performance through intelligent port configuration-Cisco Configuration Assistant includes the Cisco Smartports Advisor, which discovers devices connected in the network and recommends appropriate Cisco best practice configurations for security, availability, and QoS features on switch ports. Cisco Systems, Inc. Cisco Smartports are the 10/100 Ethernet ports in the SBCS product line switches that are managed by the CCA application. These ports can be configured by CCA for access, trunk ports and VLANs and for different devices. For a new user the config is very simple there are icons of different devices available in CCA and a novice user can simply drag the icon and drop on the port and config Cisco Smartport Advisor feature saves time by proactively recommending Cisco best practices and removes the need for network administrators to consult detailed design guides or documentation. The feature allows network administrators to configure ports more quickly; eliminates human error; and helps ensure the configuration of the switch, router, or access point is optimized for the business' applications.

is done.

Figure 2. Cisco Smartports Advisor allows roles to be assigned to specific ports and automatically optimizes performance for the attached Cisco device



- Improved IT staff efficiency and effectiveness when securing the network-Users can centrally configure security and access for Cisco Catalyst switches. Users simply choose the desired level of security (low, medium, or high) on the Security Slider in Cisco Configuration Assistant. The low setting (default) provides port security and protection against broadcast storms. The medium setting adds MAC address authentication. The high setting adds IEEE 802.1x authentication for media-level access control, providing the capability to permit or deny network connectivity and control VLAN access based on user or machine identity.

A Better Way to Deploy and Configure Business Networks

With so much depending on your network, you cannot afford to leave your business vulnerable to the performance degradation and security vulnerabilities that can arise in an improperly configured network. Cisco Configuration Assistant provides a comprehensive, easy-to-use network configuration solution. As an integral component of the Cisco Smart Business Communications System, Cisco Configuration Assistant improves the performance and security of your essential business applications, simplifies the deployment of new technologies, and dramatically improves the efficiency and effectiveness of your IT staff.
For more information about Cisco Configuration Assistant or to download the tool free of charge, visit www.cisco.com/go/configassist.

Supported Devices

Table 1 describes supported devices.

Table 1. Cisco Configuration Assistant 1.6 Managed and Supported Devices

Part Number	**Product Description**
Cisco Catalyst Express 500 Series Switches	
WS-CE500-24TT-K9	24 10/100 access ports and 2 10/100/1000BASE-T uplinks
WS-CE500-24LC-K9	20 10/100 access ports, 4 10/100 access ports with PoE ports, and 2 10/100/1000BASE-T or Small Form-Factor Pluggable (SFP) uplinks
WS-CE500-24PC-K9	24 10/100 access ports with PoE and 2 10/100/1000BASE-T or SFP uplinks
WS-CE500G-12TC-K9	8 10/100/1000BASE-T ports and 4 10/100/1000BASE-T or SFP uplinks
Cisco Catalyst Express 520 Series Switch	
WS-CE520-8PC-K9	8 10/100 access ports with PoE and 1 10/100/1000BASE-T or SFP uplinks
WS-CE520-24TT-K9	24 10/100 access ports and 2 10/100/1000BASE-T uplinks
WS-CE520-24LC-K9	20 10/100 access ports, 4 10/100 access ports with PoE ports, and 2 10/100/1000BASE-T or Small Form-Factor Pluggable (SFP) uplinks
WS-CE520-24PC-K9	24 10/100 access ports with PoE and 2 10/100/1000BASE-T or SFP uplinks
WS-CE520G-24TC-K9	24 10/100/1000BASE-T ports and 2 10/100/1000BASE-T or SFP uplinks
Cisco Unified Communications 500 Series for Small Business	
UC520-8U-4FXO-K9	8 User configuration with 4 PSTN trunks (FXO), 4 Analog ports (FXS), 8 PoE ports, 1 VIC slot for expansion Feature licenses for call control, voicemail and Cisco Unified IP Phones
UC520-8U-2BRI-K9	8 User configuration with 2 BRI trunks (BRI), 4 Analog ports (FXS), 8 PoE ports, 1 VIC slot for expansion Feature licenses for call control, voicemail and Cisco Unified IP Phones
UC520-16U-4FXO-K9	16 User configuration with 4 PSTN trunks (FXO), 4 Analog ports (FXS),

	8 PoE ports, 1 VIC slot for expansion Feature licenses for call control, voicemail and Cisco Unified IP Phones Note: requires an eight (8) port Cisco Catalyst Express 520 switch with 8 user call control feature license
UC520-16U-2BRI-K9	16 User configuration with 2 BRI trunks (BRI), 4 Analog ports (FXS), 8 PoE ports, 1 VIC slot for expansion Feature licenses for call control, voicemail and Cisco Unified IP Phones Note: requires an eight (8) port Cisco Catalyst Express 520 switch with 8 user call control feature license
UC520W-8U-4XFO-K9	8 User configuration with 4 PSTN trunks (FXO), 4 Analog ports (FXS), 8 PoE ports, 1 VIC slot for expansion Integrated Wi-Fi Access Point Feature licenses for call control, voicemail and Cisco Unified IP Phones
UC520W-8U-2BRI-K9	8 User configuration with 2 BRI trunks (BRI), 4 Analog ports (FXS), 8 PoE ports, 1 VIC slot for expansion Integrated Wi-Fi Access Point Feature licenses for call control, voicemail and Cisco Unified IP Phones
UC520W-16U-4FXO-K9	16 User configuration with 4 PSTN trunks (FXO), 4 Analog ports (FXS), 8 PoE ports, 1 VIC slot for expansion Integrated Wi-Fi Access Point Feature licenses for call control, voicemail and Cisco Unified IP Phones
UC520W-16U-2BRI-K9	16 User configuration with 2 BRI trunks (BRI), 4 Analog ports (FXS), 8 PoE ports, 1 VIC slot for expansion Integrated Wi-Fi Access Point Feature licenses for call control, voicemail and Cisco Unified IP Phones
UC520-32U-8FXO-K9	32 User configuration with 8 PSTN trunks (FXO), 4 Analog ports (FXS), 8 PoE ports, 1 VIC slot for expansion Feature licenses for call control, voicemail and Cisco Unified IP Phones Note: requires an twenty-four (24) port Cisco Catalyst Express 520 switch (WS-CE520-24PC-K9)
UC520-32U-4BRI-K9	32 User configuration with 4 BRI trunks (BRI), 4 Analog ports (FXS), 8 PoE ports, 1 VIC slot for expansion Feature licenses for call control, voicemail and Cisco Unified IP Phones Note: requires an twenty-four (24) port Cisco Catalyst Express 520 switch (WS-CE520-24PC-K9)

UC520-48U-12FXO-K9	48 User configuration with 12 PSTN trunks (FXO), 4 Analog ports (FXS), 8 PoE ports, 1 VIC slot for expansion Feature licenses for call control, voicemail and Cisco Unified IP Phones Note: requires two twenty-four (24) port Cisco Catalyst Express 520 switches (WS-CE520-24PC-K9)
UC520-48U-6BRI-K9	48 User configuration with 6 BRI trunks (BRI), 4 Analog ports (FXS), 8 PoE ports, 1 VIC slot for expansion Feature licenses for call control, voicemail and Cisco Unified IP Phones Note: requires twi twenty-four (24) port Cisco Catalyst Express 520 switches (WS-CE520-24PC-K9)
UC520-48U-T/E/F-K9	48 User configuration with T1/E1 voice interface, 4 PSTN trunks (FXO), 4 Analog ports (FXS), 8 PoE ports, 1 VIC slot for expansion Feature licenses for call control, voicemail and Cisco Unified IP Phones Note: requires two twenty-four (24) port Cisco Catalyst Express 520 switches (WS-CE520-24PC-K9)
UC520-48U-T/E/B-K9	48 User configuration with T1/E1 voice interface, 2 BRI trunks(BRI), 4 Analog ports (FXS), 8 PoE ports, 1 VIC slot for expansion Feature licenses for call control, voicemail and Cisco Unified IP Phones Note: requires two twenty-four (24) port Cisco Catalyst Express 520 switches (WS-CE520-24PC-K9)
	Cisco Unified Communications Manager Express
	Cisco Unity Express
Cisco 850 Series Integrated Services Routers	
CISCO851-K9	Cisco 851 Ethernet to Ethernet Router
CISCO851W-G-A-K9	Cisco 851 Ethernet to Ethernet Wireless Router; Americas
CISCO851W-G-E-K9	Cisco 851 Ethernet to Ethernet Wireless Router; Europe
CISCO851W-G-J-K9	Cisco 851 Ethernet to Ethernet Wireless Router; Japan
CISCO857-K9	Cisco 857 ADSL Router
CISCO857W-G-A-K9	Cisco 857 ADSL Wireless Router; U.S. and Americas

CISCO857W-G-E-K9	Cisco 857 ADSL Wireless Router; Europe
Cisco 870 Series Integrated Services Routers	
CISCO871-K9	Cisco 871 Ethernet to Ethernet Router
CISCO871W-G-A-K9	Cisco 871 Ethernet to Ethernet Wireless Router; U.S./Americas
CISCO871W-G-E-K9	Cisco 871 Ethernet to Ethernet Wireless Router; Europe
CISCO871W-G-J-K9	Cisco 871 Ethernet to Ethernet Wireless Router; Japan
CISCO876-K9	Cisco 876 ADSL over ISDN Router
CISCO876W-G-E-K9	Cisco 876 ADSL over ISDN Wireless Router
CISCO877-K9	Cisco 877 ADSL Router
CISCO877W-G-A-K9	Cisco 877 ADSL Wireless Router: U.S./Americas
CISCO877W-G-E-K9	Cisco 877 ADSL Wireless Router; Europe
CISCO878-K9	Cisco 878 G.SHDSL Router
CISCO878W-G-A-K9	Cisco 878 G.SHDSL Wireless Router; U.S./Americas
CISCO878W-G-E-K9	Cisco 878 G.SHDSL Wireless Router; Europe
Voice Interface Cards	
VIC3-2FXS/DID	2-port FXS voice/fax interface card
VIC-4FXS/DID	4-port FXS voice/fax interface card
VIC3-4FXS/DID	4-port FXS voice/fax interface card
VIC2-2FXO	2-port FXO voice/fax interface card
VIC2-4FXO	4-port FXO voice/fax interface card
VIC2-2BRI-NT/TE	2-port BRI voice/fax interface card

Cisco Mobility Express Solution	
AIR-AP521G-A-K9 AIR-AP521G-E-K9 AIR-AP521G-P-K9	Cisco 521 Wireless Express Access Point (Cisco IOS Software)
AIR-LAP521G-A-K9 AIR-LAP521G-E-K9 AIR-LAP521G-P-K9	Cisco 521 Wireless Express Access Point (Cisco Unified Wireless Network Software)
AIR-WLC526-K9	Cisco 526 Wireless Express Mobility Controller

Device Limitations

The solution supports up to 25 devices in a small office network, including:

- Five routers
- Three autonomous wireless access points
- Two wireless controllers
- Multiple Cisco IP phones (number limited to the number of switch ports in the network)

System Requirements

Table 2 describes minimum system requirements.

Table 2. Cisco Configuration Assistant 1.0 System Requirements

System Requirements	
Operating System	Windows 2000 Professional (Service Pack 3 or later) or Windows XP Professional (Service Pack 1 or later)
Disk Space	200 MB
Hardware	PC with Pentium IV
Memory	512 MB
PC Hardware	1 GHz
Screen Resolution	1024 x 768

APPENDIX-C — CISCO 500 SERIES WIRELESS MOBILITY EXPRESS CONTROLLER

The Cisco 500 Series Wireless Express Mobility Controller is designed to optimize the wireless networks of small and medium-sized businesses (SMBs). As a core element of the Cisco Mobility Express Solution, the mobility controller is built to specifically support the Cisco 500 Series Wireless Express Access Points. Together, they provide IT Managers complete visibility of the wireless network. The mobility controller automatically manages access points to reduce interference, avoid coverage gaps, maximize available bandwidth to ensure overall optimal network performance, and support advanced mobility services such as guest Internet access and voice over Wi-Fi.

Figure 4. 500 Series Controllers

The Cisco 526 Wireless Express Mobility Controller can be used with up to six access points per controller and up to two controllers per network. It harnesses the power of Cisco Lightweight Access Point Protocol (LWAPP) technology-best-in-class automatic radio optimization, mobility performance and multi-access-point management-at the capacity, simplicity, and price point appropriate for the SMB. On top of the basic transport layer, this controller supports Cisco Secure Guest Access and voice-over-WLAN advanced mobility services. Along with other products in the Smart Business Communications System, this controller uses the Cisco Configuration Assistant software rather than a command-line interface, accelerating deployment and decreasing the cost of ongoing maintenance.

Features and Benefits

Table 4 describes the features and benefits of the Cisco 526 Wireless Express Mobility Controller.

Table 4. Features and Benefits of the Cisco 526 Wireless Express Mobility Controller

Features	Benefits
Part of the Cisco Smart Business Communications System	Part of a portfolio of switching, routing, security, and voice products designed to work both individually and together as a multiproduct system to maximize the value of each product in the network.
Simplifies multi-access-point networks	Addresses issues in multi-access-point infrastructures, including scalable security, radio self-interference, and repetitive management tasks, to help ensure that multi-access-point networks operate at peak efficiency.

Streamlined management tool	Uses Cisco Configuration Assistant management software instead of a command-line interface for configuration to accelerate new and incremental deployments.
Supports Cisco LWAPP	Uses Cisco LWAPP for communication between access points and controllers to simplify deployment and follow-on management, and to automate functions required for a pervasive WLAN end-user experience.
Multi-access-point Radio Resource Management (RRM)	In builds with more than one access point, RRM coordinates access points in real time to optimize radio coverage/capacity while working around potential points of interference.
Secure authentication mechanism support	Support for a wide range of authentication mechanisms to enable scalable security architectures and minimize security interoperability issues (WEP, MAC Filtering, WPA, WPA2, WebAuth, and EAP).
Wired/wireless network virtualization	Supports the use of up to eight SSID/VLANs so that one physical WLAN infrastructure can be safely shared by different users, applications, or organizations as virtual wired/wireless networks.
Supports Cisco Secure Guest Access	With Secure Guest Access, organizations can create a virtual guest network with a login page for non-employees to get Internet access while safely partitioned from the sensitive corporate LAN.
Supports Cisco voice-over-WLAN optimization	Voice over WLAN optimization is a package of features that deliver quality of service, call admission control, and fast inter-access point hand-off to improve the quality of a wireless voice infrastructure.

Architectural Feature Comparison

With Cisco 521 Wireless Express Access Points, the Cisco Wireless Mobility Solution is an ideal fit for the SMB environment. Table 5 highlights the main architectural feature differences between consumer-grade, business-grade, and enterprise-grade WLAN solutions.

Table 5. WLAN Architectural Feature Comparison

Features	**Consumer-Grade Access Points**	**Cisco 500 Wireless Express Access Point (Standalone Mode)**	**Cisco 500 Wireless Express Access Point (Controller Mode)**	**Cisco Enterprise Unified WLAN Architecture**
Part of the Cisco Smart Business Communications	○	●	●	○

System				
Simplifies multi-access-point networks	○	◑	●	●
Cisco Configuration Assistant management tool[1]	○	●	●	○
Support for Cisco Lightweight Access Point Protocol (LWAPP)	○	○	●	●
Multi-access-point Radio Resource Management (RRM)	○	○	●	●
Support for a range of secure authentication mechanisms	○	●	●	●
Wired/wireless network virtualization	○	●	●	●
Advanced-mobility-services-ready: Cisco Secure Guest Access	○	○	●	●
Advanced-mobility-services-ready: Voice over WLAN optimization	○	○	●	●

[1] The Cisco Enterprise Unified WLAN Architecture uses Cisco Wireless Control System (WCS) Software or the command-line interface instead of the Cisco Configuration Assistant.

Product Specifications

Table 3 lists product specifications for the Cisco 526 Wireless Express Mobility Controller.

Table 6. Product Specifications for the Cisco 526 Wireless Express Mobility Controller

Item	**Specification**
Physical interfaces	2 10/100 Ethernet ports for uplink and management 2 USB console ports (future expansion)

	1 RJ-45 serial port for direct console access
Wired/switching/routing	IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX specification, and IEEE 802.1Q VLAN tagging
Management options	Cisco Configuration Assistant software (recommended) Embedded Web-based device manager Command-line interface for troubleshooting (SHO/DEBUG only) using Telnet, SSH, or console port access
Security/authentication standards	None/Open, WEP/Open, MAC Filtering, WPA/Open with EAP, WPA/Network EAP, WPA-PSK/Open with EAP, WPA-PSK/Network EAP, WPA2/AES CCMP. Supported EAP types include PEAP, LEAP, EAP-TLS, EAP-GTC, and EAP-SIM
RADIUS authentication	IEEE 802.1x RADIUS authentication. External RADIUS server required.
Multiple SSIDs	8 SSIDs supported (each access point may support multiple SSIDs) 1 SSID broadcast in SSID beacon
Support for Cisco Secure Guest Access	Allows for creation of guest SSID/VLAN through Cisco Configuration Assistant, and creation of guest user accounts and configuration of login page using Web-based device manager.
Support for voice-over-WLAN optimization	Delivers quality of service, call admission control, fast inter-access point hand-off, and other optimization features to improve the quality of a wireless voice infrastructure.

Ordering Information

Table 4 provides ordering information for the Cisco 526 Wireless Express Mobility Controller. To place an order, visit the Cisco Ordering Website:
http://www.cisco.com/en/US/ordering/index.shtml

Table 4. Ordering Information for Cisco 526 Wireless Express Mobility Controller

Part Number	**Product Name**
AIR-WLC526-K9	Cisco 526 Wireless Express Mobility Controller for up to six Cisco 500 Series Wireless Express Access Points

APPENDIX-D — CISCO 500 SERIES UNIFIED COMMUNICATION

The Cisco Unified Communications 500 Series is an all-in-one unified communications solution that integrates voice, data, video, security, wireless, and management into one platform. It brings unified communications to small businesses and organizations by providing a simplified, affordable solution that is easy to configure, deploy, and manage. By combining call control, messaging, and mobility into one device, the Cisco Unified Communications 500 Series eliminates the added costs of multiple servers and provides a solution that is easy to set up and manage at a lower price point.

Figure 4: CISCO UNIFIED COMUNNICATIONS 500 SERIES

Cisco Unified Communications 500 Series for Small Business, a critical part of the Cisco Smart Business Communications System, is a unified communications solution for small businesses that provides voice, data, voicemail, Automated Attendant, video, security, and wireless capabilities while integrating with existing desktop applications such as calendar, e-mail, and customer relationship management (CRM) programs. This easy-to-manage platform uses business-class, proven unified communications technologies to full advantage and supports flexible deployment models based on your needs-a wide array of IP phones, public switched telephone network (PSTN) interfaces, and Internet connectivity.

Core Components:

- Cisco Unified IP phones, including wireless handsets and Session Initiation Protocol (SIP) phones
- Cisco Unified Communications Manager Express for call processing
- Cisco Unity® Express for voice messaging and Automated Attendant
- LAN switching: Integrated and expandable through Cisco Catalyst® Express 520 Series Switches
- Security, firewall, and VPN capabilities
- Optional wireless LAN capability
- Cisco Configuration Assistant for GUI-based customization of the solution

Cisco Unified IP Phones

Cisco provides a complete range of Cisco Unified IP phones and communications devices designed to take full advantage of converged voice and data networks, and these devices offer the convenience and user friendliness found in business phones. Cisco Unified IP phones can help improve productivity by meeting the needs of different users throughout the organization.
The Cisco Unified IP phone portfolio provides the following:

- IP phones with LCD displays, including dynamic soft keys for call features and functions
- Support for information services, including Extensible Markup Language (XML) capabilities to extend IP phone systems to give IP phone users access to a variety of information such as stock quotes, employee directories, and Web-based content

Cisco Unified IP phones lead the IP communications device market and provide a complete IP phone system portfolio with ease of use, superior audio quality, increased accessibility for people with disabilities, ergonomic physical design, advanced services, and features.

The IP phone portfolio includes options for use from wherever the user is located: the company lobby, the manufacturing floor, the executive suite, at home, on the road, or in branch offices (Figure 2).

Figure 5. Cisco Unified IP Phone Portfolio

Cisco Unified Communications Manager Express

Cisco Unified Communications Manager Express is a Cisco IOS® Software solution embedded in the Cisco Unified Communications 500 Series appliance that provides call processing for Cisco Unified IP phones. Simple to deploy, administer, and maintain, Cisco Unified Communications Express is a reliable, feature-rich telephony solution.

Cisco Unity Express

Embedded Cisco Unity Express enables voicemail, desktop messaging, and Automated Attendant services for increased customer service and rich employee communications experience.

Cisco Unified CallConnectors for Desktop Applications

The Cisco Unified Communications 500 Series integrates with common Windows desktop applications to give small business owners access to productivity gains once available only to large businesses. With Cisco Unified CallConnectors, customers can integrate their Cisco Unified IP phones with common applications including Microsoft Outlook, Internet Explorer, Microsoft Dynamics CRM, or Salesforce.com CRM.

Integrated Network Firewall and Security

Security is a fundamental building block of any network, and Cisco products play an important role in embedding security at the customer's access edge. The Cisco IOS Firewall is a stateful-inspection firewall available with the Cisco Unified Communications 500 Series. Built from market-leading Cisco PIX® Firewall technologies, Cisco IOS Firewall is supported on the Cisco Unified Communications 500 Series platform as a base feature. Cisco IOS Firewall is an ideal single-box solution for protecting the WAN entry point into the network.

Virtual Private Networking

VPNs carry private data over a public network and extend remote access to users over a shared infrastructure. VPNs maintain the same security and management policies as private networks and are the most cost-effective means of establishing point-to-point connection between remote users and a central network. VPNs have been the fastest-growing form of network connectivity, and Cisco takes this approach to a new standard by making VPN functions an integral part of the Cisco Unified Communications offering. The Cisco Unified Communications 500 Series includes built-in hardware-based encryption acceleration that offloads IP Security (IPsec), Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Triple DES (3DES) encryption and VPN processes to provide increased VPN throughput with minimal effect on the Cisco Unified Communications 500 Series CPU.

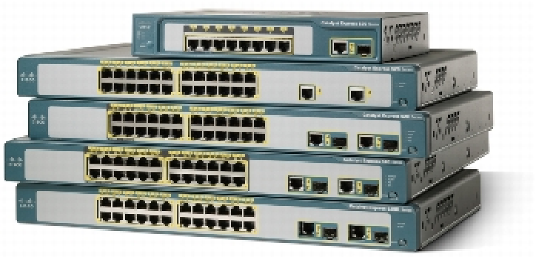
APPENDIX-E — CISCO CATALYST EXPRESS 520 SERIES SWITCHES

Cisco Catalyst Express 520 Series Switches are a family of fixed-configuration, Layer 2 managed Ethernet switches that provide the reliability, scalability, and rich feature set your business needs in a cost-effective, easy-to-manage platform. Designed specifically for organizations with fewer than 250 employees, the solutions provide:

- Wire-speed Fast Ethernet and Gigabit Ethernet connectivity
- Power over Ethernet (PoE) to provide 15.4 Watts simultaneously on all PoE ports
- Quality-of-service (QoS) intelligence to prioritize delay-sensitive traffic
- Robust integrated security to protect management traffic
- Simple deployment, centralized management, and troubleshooting
- Scalability to continually incorporate new applications and services over time
- Easy integration with established architectures without requiring major upgrades to the network infrastructure
- Limited Lifetime Warranty and free Cisco IOS® Software updates

For businesses that have been using basic, unmanaged network switches but now need higher performance, increased reliability, and a more advanced feature set, the Cisco Catalyst Express 520 Series offers an ideal solution.
Figure 1 shows Cisco Catalyst Express 520 Series Switches.

Figure 1. Cisco Catalyst Express 520 Series Switches



Configurations

Table 1 highlights the various configurations available in the Cisco Catalyst Express 520 Series.

Table 1. Cisco Catalyst Express 520 Series Configurations

Product Name (SKU)	**Description**
Cisco Catalyst Express 520-8PC-K9 Switch (WS-CE520-8PC-K9)	• 8 10/100 access ports with PoE • 1 10/100/1000BASE-T or Small Form-Factor Pluggable (SFP) uplink
Cisco Catalyst Express 520-24TT Switch (WS-CE520-24TT-K9)	• 24 10/100 access ports for desktop connectivity • 2 10/100/1000BASE-T ports for uplink or server connectivity

Cisco Catalyst Express 520-24LC Switch (WS-CE520-24LC-K9)	• 20 10/100 access ports for desktop connectivity • 4 10/100 access ports with PoE for desktop, wireless access point, IP telephony, or closed-circuit TV camera connectivity • 2 10/100/1000BASE-T or SFP ports for flexible uplink or server connectivity
Cisco Catalyst Express 520-24PC Switch (WS-CE520-24PC-K9)	• 24 10/100 access ports with PoE for desktop, wireless, IP telephony, or closed-circuit TV camera connectivity • 2 10/100/1000BASE-T or SFP ports for flexible uplink or server connectivity
Cisco Catalyst Express 520G-24TC Switch (WS-CE520G-24TC-K9)	• 24 10/100/1000BASE-T ports for uplink or server connectivity • 2 10/100/1000BASE-T or SFP ports for flexible uplink or server connectivity
Cisco Catalyst Express 520 Spare Rack Mount Kit (RCKMNT-CATEXP=)	Cisco Catalyst Express 520 spare rack mount kit

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax:408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax:31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax:408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Printed in the USA